

目次

[Kaspersky Endpoint Security の概要](#)

[このバージョンの新機能](#)

[Kaspersky Security Center 管理ツールによる Kaspersky Endpoint Security 機能の比較](#)

[本製品のインストールとアンインストール](#)

[配布キット](#)

[システム要件](#)

[インストールの準備](#)

[Kaspersky Endpoint Security のインストール](#)

[製品の使用準備](#)

[Kaspersky Endpoint Security のアンインストール](#)

[本製品の初回起動](#)

[Kaspersky Endpoint Security のインターフェイス](#)

[メインウインドウ](#)

[Kaspersky Endpoint Security のアイコン](#)

[本製品の設定ウインドウ](#)

[通知について](#)

[Kaspersky Endpoint Security のライセンス](#)

[使用許諾契約書について](#)

[ライセンスについて](#)

[定額制サービスについて](#)

[ライセンス証明書について](#)

[ライセンス情報について](#)

[アクティベーションコードについて](#)

[ライセンス情報ファイルについて](#)

[データ提供について](#)

[Kaspersky Endpoint Security のアクティベーション](#)

[ライセンス情報を表示する](#)

[ライセンスと定額制サービスの管理](#)

[ワークステーションのライセンス種別に応じた製品機能の比較](#)

[標準タスクの実行](#)

[本製品の起動と終了](#)

[コンピュータの保護ステータスの表示](#)

[インストールされているコンポーネントの動作状況の表示](#)

[保護機能の無効化および再開](#)

[プロテクションセンターの使用](#)

[スキャンタスクの実行](#)

[スケジュール済みスキャンタスクの自動起動の設定](#)

[定義データベースのアップデート](#)

[ファイルアクセスがブロックされた場合の操作](#)

[削除または駆除されたファイルの復元](#)

[製品の動作レポートの表示](#)

[通知ウインドウが表示された場合の操作](#)

[製品の詳細設定](#)

[コンピュータの保護対象](#)

[ファイル脅威対策](#)

[ウェブ脅威対策](#)

[メール脅威対策](#)

[ネットワーク脅威対策](#)

[ファイアウォール](#)

[ふるまい検知](#)

[スキャン](#)

[アップデートタスク](#)

[ローカルタスク](#)

[外部ディスクのスキャンタスク](#)

[バックアップ](#)

[レポート](#)

[Managed Detection and Response](#)

[Endpoint Detection and Response \(KATA\)](#)

[Endpoint Detection and Response Optimum](#)

[Endpoint Detection and Response Optimum との連携](#)

[セキュリティ侵害インジケータのスキャン](#)

[ファイルの隔離](#)

[ファイルの取得](#)

[ファイルの削除](#)

[プロセスを開始](#)

[プロセスの終了](#)

[実行防止](#)

[コンピュータネットワークの分離](#)

[Cloud Sandbox](#)

[FileVault ディスク暗号化](#)

[パスワードによる保護](#)

[脆弱性攻撃ブロック](#)

[修復エンジン](#)

[ウェブコントロール](#)

[デバイスコントロール](#)

[Kaspersky Security Network に参加する](#)

[製品コンポーネントの整合性をチェックする](#)

[Kaspersky Security Center 管理コンソールからの製品の管理](#)

[企業ネットワークに Kaspersky Endpoint Security を導入する](#)

[Kaspersky Endpoint Security バージョン 11.1 以降をバージョン 12.2 にアップデート](#)

[Kaspersky Endpoint Security のリモートインストールの準備](#)

[Kaspersky Endpoint Security 管理プラグインをインストールする](#)

[ローカルでネットワークエージェントをインストールする](#)

[Apple Remote Desktop を使用してネットワークエージェントをインストールする](#)

[Kaspersky Security Center を使用してネットワークエージェントをインストールする](#)

[SSH プロトコルを使用してネットワークエージェントをインストールする](#)

[ローカルでネットワークエージェントをアンインストールする](#)

[コマンドラインからのネットワークエージェントの管理](#)

[リモートコンピュータ上のネットワークエージェントの開始または停止](#)

[クライアントコンピュータと管理サーバー間の接続の手動確認: Klnagchk ユーティリティ](#)

[リモートコンピュータから管理サーバーへの手動接続: Klmover ユーティリティ](#)

[ネットワークエージェントをアンインストールする](#)

[Kaspersky Endpoint Security のインストールとアンインストール](#)

[SSH プロトコルを使用したインストール](#)

[Kaspersky Security Center を使用したインストール](#)

[インストールパッケージの作成](#)

[Kaspersky Security Center を使用したアンインストール](#)

[Kaspersky Security Center からの製品の開始と停止](#)

[タスクの作成と管理](#)

[タスクの作成](#)

[タスクの手動での開始と停止](#)

[タスクのインポートおよびエクスポート](#)

[タスクの表示](#)

[タスク固有設定の管理](#)

[ポリシーの作成と管理](#)

[ポリシーの作成](#)

[ポリシーのリストを表示する](#)

[ポリシーの設定](#)

[ポリシーのステータスを変更する](#)

[KLP ファイルにポリシーをエクスポートする](#)

[KLP ファイルからポリシーをインポートする](#)

[ポリシーのプロファイルの作成と管理](#)

[検知したオブジェクトのレポートを生成する](#)

[暗号化されたディスクの回復キーを取得する](#)

[Kaspersky Security Center Web コンソールおよび Cloud コンソールを経由する製品のリモート管理](#)

[Kaspersky Endpoint Security Web プラグインをインストールする](#)

[ポリシーの作成](#)

[先進の脅威対策の設定](#)

[脅威対策の設定](#)

[ファイル脅威対策の設定](#)
[ウェブ脅威対策の設定](#)
[ネットワーク脅威対策の設定](#)
[セキュリティコントロールの設定](#)
[データ暗号化の設定](#)
[Detection and Response の設定](#)
[Managed Detection and Response の設定](#)
[Endpoint Detection and Response の設定](#)
[Endpoint Detection and Response \(KATA\) の設定](#)
[アップデートの設定](#)
[詳細設定](#)
[タスクの作成](#)
[スキャンタスクの設定の編集](#)
[ライセンスの追加タスクの設定の編集](#)
[アップデートタスクの設定](#)
[暗号化されたドライブの回復キーを取得する](#)
[コマンドラインからの製品の管理](#)
[コマンドラインヘルプの表示](#)
[マルウェアスキャンの実行](#)
[製品のアップデート](#)
[前回のアップデートのロールバック](#)
[コンポーネントまたはタスクの開始と停止](#)
[コンポーネントまたはタスクのステータスと統計の表示](#)
[保護設定のエクスポート](#)
[本製品のアクティベーション](#)
[システム機能拡張のインストール](#)
[ネットワーク接続の設定](#)
[ライセンス情報の削除](#)
[コマンドラインのリターンコード](#)
[本製品の終了](#)
[本製品のアンインストール](#)
[Detection and Response 管理コマンド](#)
[実行防止の管理](#)
[ネットワーク分離の管理](#)
[テクニカルサポートへの問い合わせ](#)
[テクニカルサポートのご利用方法](#)
[カスペルスキーカンパニーアカウントによるテクニカルサポート](#)
[テクニカルサポート用の情報収集](#)
[トレースファイルの使用](#)
[トレースファイルの作成](#)
[製品の情報源](#)
[付録](#)
[既知の問題と制限](#)
[拡張子に応じてスキャンされるオブジェクトのリスト](#)
[ファイルおよびフォルダへのパスのマスク](#)
[IOC ファイルの要件](#)
[実行防止用にサポートされているスクリプトインタープリタの実行を設定](#)
[Kaspersky Endpoint Security の証明書を Mozilla Firefox 証明書ストアに追加する方法](#)
[サードパーティ製のコードに関する情報](#)
[商標に関する通知](#)

Kaspersky Endpoint Security の概要

Kaspersky Endpoint Security は、macOS のコンピュータを、マルウェアやセキュリティ上のその他の脅威から保護します。

ファイル脅威対策

ファイル脅威対策は、ファイルへのアクセスを補足し分析することで、コンピュータのファイルシステムをリアルタイムで保護します。[詳細](#)

ウェブ脅威対策

ウェブ脅威対策は、Safari、Google Chrome™、Firefox™ で HTTP および HTTPS プロトコルを使用してコンピュータが送受信する情報を保護します。[詳細](#)

メール脅威対策

メール脅威対策は、送受信メールの添付ファイルをスキャンして、マルウェアやその他の脅威を検出します。このコンポーネントは、定義データベース、Kaspersky Security Network クラウドサービス、ヒューリスティック分析を利用してコンピュータを保護します。[詳細](#)

ネットワーク脅威対策

ネットワーク脅威対策は、オペレーティングシステムへの侵入を防止します。このコンポーネントは、サイバー攻撃者（ポートスキャン攻撃や総当たり攻撃を使用）およびこのような攻撃者がインストールするマルウェア（個人情報を攻撃者に送信するマルウェアを含む）から保護します。[詳細](#)

ファイアウォール

インターネットまたはローカルネットワークでの作業時に、ファイアウォールによって、コンピュータへの不正な接続がブロックされます。ファイアウォールは、コンピュータ上のアプリケーションのネットワーク動作も制御します。これにより、個人情報の盗難やその他の攻撃から企業 LAN を保護できます。このコンポーネントは、定義データベース、Kaspersky Security Network クラウドサービス、および事前定義されたネットワークルールを使用してコンピュータを保護します。[詳細](#)

ふるまい検知

ふるまい検知コンポーネントは、コンピュータ上のアプリケーションの動作に関する情報を受信し、この情報を他の保護コンポーネントに提供して、パフォーマンスを向上させます。また、マルウェア活動への対応として、選択された処理を実行します。[詳細](#)

脆弱性攻撃ブロック

脆弱性攻撃ブロックは、コンピュータ上の脆弱性を悪用して管理者権限を取得したり悪意のある活動を実行しようとするプログラムコードを検知します。[詳細](#)

修復エンジン

修復エンジンを使用すると、マルウェアがオペレーティングシステム内で行った処理をロールバックできます。[詳細](#)

スキャン

Kaspersky Endpoint Security により、指定したスキャン範囲に対して、オンデマンドでマルウェアやコンピュータのセキュリティに対するその他の脅威を検知し、無害化できます。Kaspersky Endpoint Security では、コンピュータの完全スキャン、重要領域の簡易スキャン、指定した範囲のスキャンを実行できます。[詳細](#)

アップデート

Kaspersky Endpoint Security は、カスペルスキーのアップデートサーバ、ディストリビューションポイント、またはシステム管理者が指定するその他のアップデート元から定義データベースとソフトウェアモジュールをアップデートします。また、アップデートされたすべてのファイルのバックアップコピーを作成して、前回のアップデート前の状態にロールバックできるようにします。[詳細](#)

バックアップ

Kaspersky Endpoint Security は、感染したファイルを駆除または削除する前にバックアップコピーを作成し、復元できるようにします。[詳細](#)

レポート

Kaspersky Endpoint Security では、製品コンポーネントに関連するイベントと動作に関するレポートが作成されます。[詳細](#)

通知

Kaspersky Endpoint Security では、通知を使用して、Kaspersky Endpoint Security の動作中の特定のイベントをユーザに知らせます。通知では音が鳴ることもあります。[詳細](#)

プロテクションセンター

Kaspersky Endpoint Security では、保護ステータスのメッセージがプロテクションセンターに表示されます。プロテクションセンターには、その時点でのコンピュータの保護ステータスに関する情報と、コンピュータのセキュリティに対する問題および脅威の解決方法が表示されます。[詳細](#)

Kaspersky Security Center を使用した本製品のリモート管理

Kaspersky Endpoint Security がインストールされたコンピュータの保護をリモートで管理できます。次のことが可能です：コンピュータの保護の現在のステータスに関する情報の受信、リモートでの問題の解決、コンピュータのセキュリティ上の脅威への対応、保護機能（ファイル脅威対策、ウェブ脅威対策、ネットワーク脅威対策、ふるまい検知）の有効化と無効化、ウェブコントロール、Managed Detection and Response、Endpoint Detection and Response、Endpoint Detection and Response (KATA) の有効化と無効化、スキャンタスクの実行、定義データベースのアップデート、起動ディスクの暗号化の実行、Kaspersky Endpoint Security のライセンスとサブスクリプションの管理。次のツールを使用して、Kaspersky Endpoint Security を管理できます：

- Kaspersky Security Center 管理コンソール。[詳細](#)
- Kaspersky Security Center Web コンソールおよび Cloud コンソール。[詳細](#)

注意：Kaspersky Endpoint Security がサポートする機能は、使用する管理ツールによって異なります。

FileVault ディスク暗号化

Kaspersky Endpoint Security により、FileVault ディスク暗号化のリモート管理が可能です。暗号化により、ユーザのコンピュータの起動ディスクに保存された機密データに対する不正なユーザアクセスを防止できます。

注意：FileVault ディスク暗号化機能は、Kaspersky Security Center 10 SP3 以降で使用できます。詳しくは、カスペルスキーのテクニカルサポートにお問い合わせください。

ウェブコントロール

ユーザによる Web サイトのアクセスをリモート管理できます。特定の URL、または URL のグループをブロックまたは許可の対象に設定できます。また、特定のカテゴリに属する Web サイトをその内容に基づいてブロックまたは許可の対象に設定できます。[詳細](#)

デバイスコントロール

デバイスコントロールによって、コンピュータにインストールされているデバイスまたはコンピュータに接続されているデバイスへのユーザアクセスが管理されます。これにより、こうしたデバイスの接続時にコンピュータを感染から保護し、データの損失や漏えいを防ぐことができます。[詳細](#)

Managed Detection and Response

Managed Detection and Response コンポーネントは、Kaspersky Managed Detection and Response サービスと対話します。このサービスは、組織を標的とする脅威を継続的に探索、検知、排除します。[詳細](#)

Endpoint Detection and Response

Endpoint Detection & Response コンポーネントは、Kaspersky Endpoint Detection and Response ソリューションとの対話を簡易化します。このソリューションは、脅威の自動検知と、これらの脅威に対応する能力を組み合わせ、新種の脆弱性攻撃、ランサムウェア、ファイルレス攻撃、正規のシステムツールを使用した方法などの高度な攻撃に対抗します。[詳細](#)

Endpoint Detection and Response (KATA)

Endpoint Detection & Response (KATA) コンポーネントは、Kaspersky Anti Targeted Attack Platform ソリューションとの対話を簡易化します。このソリューションは、標的型攻撃、高度な持続的脅威、ゼロデイ攻撃などの高度な脅威を迅速に検知します。[詳細](#)

このバージョンの新機能

このヘルプは、Kaspersky Endpoint Security for Mac バージョン 12.2 用です。

新機能と強化点は次の通りです：

- 新しい macOS 27 Golden Gate に対応しました。
- 新しい macOS 26 Tahoe に対応しました。

- メール脅威対策、デバイスコントロール、ファイアウォール、修復エンジン、脆弱性攻撃ブロックコンポーネントを追加しました。
- Kaspersky Endpoint Security から Managed Detection and Response コンポーネントをアクティベートできるようになりました。
- アラートの詳細に対する応答処理の可視性が向上しました。
- Web コンソールでふるまい検知コンポーネントを管理できるようになりました。
- アラートの概要を追加しました。
- オブジェクトが重要なシステムオブジェクトである場合、応答処理が実行される前に通知されるようになりました。
- IOC スキャン タスク設定を作成または編集するときに、Web コンソールで IOC ファイルを直接編集できるようになりました。
- 検出されたオブジェクトをアラートの詳細から隔離できるようになりました。
- ネットワーク分離タスクの制限された動作に関する警告を追加しました。
- 一部の不具合を修正し、機能を改善しました。

Kaspersky Security Center 管理ツールによる Kaspersky Endpoint Security 機能の比較

Kaspersky Endpoint Security がサポートする機能は、使用する管理ツールによって異なります（下の表を参照）。

次のツールを使用して、Kaspersky Endpoint Security を管理できます：

- Kaspersky Security Center 管理コンソール。Kaspersky Security Center 管理者のワークステーションにインストールされた Microsoft 管理コンソール（MMC）スナップイン。
- Kaspersky Security Center Web コンソール。管理サーバーにインストールされている Kaspersky Security Center のコンポーネント。管理サーバーにアクセスできるすべてのコンピュータ上のブラウザを使用して、Web コンソールを操作できます。
- Kaspersky Security Center Cloud コンソール。クラウドバージョンの Kaspersky Security Center。

Kaspersky Endpoint Security 機能の比較

機能	Kaspersky Security Center		
	管理コンソール	Web コンソール	Cloud コンソール
先進の脅威対策			
Kaspersky Security Network	✓	✓	✓
ふるまい検知	✓	✓	
脆弱性攻撃ブロック	✓	✓	
修復エンジン	✓	✓	
脅威対策			
ファイル脅威対策	✓	✓	✓
ウェブ脅威対策	✓	✓	✓
ネットワーク脅威対策	✓	✓	✓
メール脅威対策	✓	✓	
ファイアウォール	✓	✓	
セキュリティコントロール			
ウェブコントロール	✓	✓	✓
デバイスコントロール	✓	✓	
データ暗号化			
FileVault ディスク暗号化	✓	✓	✓
回復キー	✓	✓	✓
Detection and Response			
Managed Detection and Response	✓	✓	✓
Endpoint Detection and Response		✓	

Endpoint Detection and Response (KATA)	✓	✓	✓
タスク			
ライセンスの追加	✓	✓	✓
アップデート	✓	✓	✓
簡易スキャン	✓	✓	
ロールバック	✓	✓	✓
スキャン	✓	✓	✓

本製品のインストールとアンインストール

配布キット

Kaspersky Endpoint Security のインストールパッケージが含まれる配布キットには、次のファイルが含まれています：

- 使用可能な方法のいずれかによってアプリケーションをインストールするのに必要な各ファイル。
- [使用許諾契約書](#)を含む license_<loc>.txt ファイル。
使用許諾契約書では、製品使用の条件が指定されます。

圧縮されたインストールパッケージのファイルにアクセスするには、インストールパッケージを解凍してください。

システム要件

Kaspersky Endpoint Security のシステム要件は、次の通りです：

- プロセッサ種別：Intel、Apple シリコン
- 4 GB 以上のメモリ
- 5 GB 以上のディスク空き容量
- macOS 13、14、15、26、27 のオペレーティングシステム
- インターネット接続

対応ブラウザ：

- Safari
- Chrome
- Firefox

Kaspersky Endpoint Security は、次の仮想化ツールと互換性があります：

- Parallels Desktop 16 for Mac Business Edition 以降
- VMware Fusion™ 11.5 Professional
- VMware Fusion 12 Professional
- VMware Fusion 13 Pro

MDM プロファイルは、Jamf および Apple のサーバーに導入できます。それ以外のサーバーを使用する場合は、[テクニカルサポートサイト](#) (ナレッジベース) を参照してください。

Kaspersky Security Center を使用すると、Kaspersky Endpoint Security をリモートで管理できます。Kaspersky Security Center 管理コンソールの管理プラグインと Kaspersky Security Center Webコンソールの Web プラグインを使用して Kaspersky Endpoint Security を管理するには、Kaspersky Security Center 14.2 以降が必要です。

注意： Kaspersky Security Center を使用して Kaspersky Endpoint Security for Mac 12.2 を管理するには、ネットワークエージェントのバージョン 15 をリモートコンピュータにインストールする必要があります。

インストールの準備

Kaspersky Endpoint Security をコンピュータにインストールする前に、次を実行することを推奨します：

- コンピュータが [システム要件](#) を満たしていることを確認します。
- カスペルスキー インターネット セキュリティ for Mac などのマルウェア対策製品を削除し、システム上の競合を防止してパフォーマンスを最大化します。

注意： 本製品のリモートインストール前に、圧縮ファイル KES_for_macOS11_and_later.zip をカスペルスキーのテクニカルサポートサイトからダウンロードし、Apple Remote Management ツールを使用して設定プロファイル KES_for_macOS11_and_later_profile.mobileconfig をクライアントコンピュータへ適用しておくことを推奨します。これにより、本製品に次の権限が許可されます：カーネル機能拡張とシステム機能拡張のインストール、フルディスクアクセス、ネットワーク接続の設定編集。設定プロファイルとその他のオプションの詳細は、[テクニカルサポートサイト](#)  を参照してください。

Kaspersky Endpoint Security のインストール

重要： このガイドに記載されている方法でのみ、Kaspersky Endpoint Security をインストールすることを推奨します。

Kaspersky Endpoint Security は次のいずれかの方法でインストールできます：

- カスペルスキーの **Web** サイトからダウンロードできる配布キットを使用してローカルで。
 - Apple Remote Desktop を使用してリモートで。
 - [Kaspersky Security Center](#) の管理コンソールを使用してリモートで。
 - Kaspersky Security Center Web コンソールまたは Kaspersky Security Center Cloud コンソールを経由してリモートで。
- Kaspersky Security Center Web コンソールを使用しているカスペルスキー製品の導入に関する詳細は、[Kaspersky Security Center のヘルプ](#)  を参照してください。Kaspersky Security Center Cloud コンソールを使用したカスペルスキー製品の導入に関する詳細は、[Kaspersky Security Center Cloud コンソールのヘルプ](#)  を参照してください。

[Kaspersky Endpoint Security の標準インストールを実施する](#)

1. 配布キットの ZIP ファイルを展開します。
2. 展開したアーカイブにある dmg ファイルを開きます。
3. 表示されたウィンドウで、**[インストール]** をダブルクリックします。
Kaspersky Endpoint Security のインストールアシスタントが開きます。
4. **[インストール]** をクリックします。
5. インストールアシスタントの手順に従って、インストールを完了します。

インストールが完了すると、Kaspersky Endpoint Security が自動的に起動します。コンピュータを再起動する必要はありません。

注意： このインストール方法を使用すると、Endpoint Detection and Response (KATA)、Endpoint Detection and Response (Optimum)、および Cloud Sandbox コンポーネントはインストールされません。

[Kaspersky Endpoint Security のカスタムインストールを実行する](#)

1. 配布キットの ZIP ファイルを展開します。
2. 展開したアーカイブにある dmg ファイルを開きます。
3. 表示されたウィンドウで、**[インストール]** をダブルクリックします。
Kaspersky Endpoint Security のインストールアシスタントが開きます。
4. **[カスタマイズ]** をクリックし、インストールしないコンポーネントに隣接するチェックボックスをオンまたはオフにし、**[続行]** をクリックします。
5. インストールアシスタントの手順に従って、インストールを完了します。

インストールが完了すると、Kaspersky Endpoint Security が自動的に起動します。コンピュータを再起動する必要はありません。

[Apple Remote Desktop を使用して本製品をインストールする](#)

1. Mac で、[Apple メニュー] → [システム設定] → [一般] → [共有] の順に選択します。
 2. [リモートマネージメント] をオンにします。
 3. サーバとして使用する Mac に、Apple Remote Desktop をインストールします。Apple Remote Desktop の詳細は、[Apple のサポートサイト](#)  を参照してください。
 4. Apple Remote Desktop を開きます。
 5. [Remote Desktop] ウィンドウで、左側の [スキャナ] をクリックし、Kaspersky Endpoint Security をインストールするデバイスを選択します。
 6. [インストール] をクリックします。
 7. 管理者の認証情報を要求されたら、管理者名とパスワードを入力して [追加] をクリックします。
 8. + をクリックし、Kaspersky Endpoint Security インストールパッケージの dmg ファイルを選択します。
 9. [インストール] をクリックします。
- 選択したデバイスへの Kaspersky Endpoint Security のインストールが開始されます。

製品の使用準備

Kaspersky Endpoint Security のインストールが完了したら、次の操作を実行できます：

- [Kaspersky Endpoint Security をアクティベートします](#)。Kaspersky Endpoint Security をアクティベートするとコンピュータの保護が開始され、定義データベースおよびソフトウェアモジュールの定期的なアップデート、マルウェアスキャンタスクの実行、テクニカルサポートへのリクエストの送信が可能になります。

Managed Detection and Response コンポーネントは、[Kaspersky Security Center 管理コンソール](#)または [Web コンソール](#)で個別に有効化されます。

Endpoint Detection and Response コンポーネントが現在のライセンスでサポートされていない場合は、Kaspersky Endpoint Detection and Response を個別にアクティベートする必要があります。

- [コンピュータの保護ステータスの確認](#)
- [Kaspersky Endpoint Security のアップデート](#)
- [コンピュータにマルウェアがないかどうかスキャンします](#)。

Kaspersky Endpoint Security のアンインストール

1. 配布キットの DMG ファイルを開きます。
2. 配布キットの内容のウィンドウで、[アンインストール] をダブルクリックします。
Kaspersky Endpoint Security のアンインストーラが起動します。
3. アンインストーラのウィンドウで、[削除] をクリックします。
4. 管理者の認証情報の入力画面で管理者の名前とパスワードを入力し、Kaspersky Endpoint Security のアンインストールを確定します。
Kaspersky Endpoint Security のアンインストールが開始されます。
5. アンインストールの完了の情報を確認し、[終了] をクリックしてアンインストーラを終了します。

Kaspersky Endpoint Security がコンピュータからアンインストールされます。製品のアンインストール後、コンピュータを再起動する必要はありません。

本製品の初回起動

Kaspersky Endpoint Security は、コンピュータへのインストール後すぐに起動します。Mac の保護をすぐに開始するために、基本的な設定の指定が要求されます。

- マルウェア、ネットワーク攻撃、インターネット上の脅威から Mac を保護するのに必要な権限を本製品に対して許可してください。
許可する権限の詳細は、(?) をクリックしてください。
- [Kaspersky Endpoint Security をアクティベートします。](#)

注意：本製品の基本的な設定には、インターネット接続が必要です。

[Kaspersky Endpoint Security の初回起動](#)

1. **「必須の保護機能」** ウィンドウで次の操作を実行し、ファイル脅威対策とウェブ脅威対策が正しく動作することを確認します：

- Kaspersky Endpoint Security を正常に動作させるために、Mac 上の全ファイルのスキャンを許可します。許可するには、**「フルディスクアクセス」** の隣にある **「許可」** をクリックし、画面の指示に従います。
- Mac に損害が及ぶ前に Kaspersky Endpoint Security で URL とネットワークパケットを検査する場合、システム機能拡張をインストールします。インストールするには、**「システム機能拡張」** の隣にある **「インストール」** をクリックし、画面の指示に従います。
- システム機能拡張を適切に動作させるには、ネットワークコンテンツのフィルタリングを許可します。許可するには、**「ネットワークコンテンツのフィルタ機能」** に隣接する **「許可」** をクリックし、画面の指示に従います。
- マルウェアとインターネット上の脅威が暗号化された HTTPS トラフィックにないかどうかを検査する場合は、信頼済み証明書をインストールします。インストールするには、**「信頼済み証明書」** に隣接する **「インストール」** をクリックし、画面の指示に従います。

重要：この権限を許可しないと、Kaspersky Endpoint Security が正常に動作しません。**「必須の保護機能」** ウィンドウで、すべての権限を許可する必要があります。

2. **「続行」** をクリックします。

メインウィンドウが表示されます。

Kaspersky Endpoint Security のインターフェイス

メインウィンドウ

[メインウィンドウを開く](#)

メニューバーにある本製品のアイコンをクリックし、**「Kaspersky Endpoint Security」** を選択します。

Kaspersky Endpoint Security のメインウィンドウには、主要機能へのアクセスを提供するインターフェイス要素が含まれています。

メインウィンドウは 2 つの部分に分かれています：

- 左側には、本製品の機能を移動して簡単にアクセスできるサイドバーが表示されます。
- 中央部分には、サイドバーで選択したセクションの内容が表示され、そこでデータを管理することができます。

サイドバー

本製品のメインウィンドウのサイドバーには次のオプションがあります：

 監視	クリックすると、 「監視」 ページが開きます。このページには、Kaspersky Endpoint Security がコンピュータを保護するために実行している動作に関する情報が表示されます。
 プロテクションセンター	クリックすると、コンピュータの保護ステータスが表示されます。 詳細
 セキュリティ	クリックすると、インストールされているコンポーネントの動作ステータスが表示されます。 詳細
 スキャン	スキャンタスクを管理します。 詳細
 アップデート	アップデートタスクを管理します。 詳細

[監視] ページの管理項目

[監視] ページには、[保護ステータスインジケータ](#)が表示され、Kaspersky Endpoint Security がコンピュータを保護するために実行している内容に関する情報が表示されます。また、次の管理項目が含まれます。

プロテクションセンター	コンピュータ保護の問題について通知します。 詳細
レポート	本製品、個々の機能、タスクの動作中に発生したイベントを表示できます。 詳細
バックアップ	削除した感染ファイルの保存コピーのリストを表示できます。 詳細 詳細
脅威検知	Kaspersky Endpoint Security が適用する脅威検知技術に関する情報と、これらの技術により検知された脅威の数を表示できます。
Kaspersky Security Network	Kaspersky Endpoint Security と Kaspersky Security Network の間の接続のステータスと、Kaspersky Security Network のグローバルな統計を表示します。

Kaspersky Endpoint Security のアイコン

Kaspersky Endpoint Security がインストールされると、メニューバーに本製品のアイコンが表示されます。製品をアクティベートすると、このアイコンから製品のステータスを判断することができます。製品アイコンがアクティブである（**k**）場合、すべてまたは一部の保護コンポーネントが有効になっていることを表します。製品アイコンがアクティブではない（**K**）場合、すべての保護コンポーネントが無効です。

[製品アイコンのメニューを開く](#)

メニューバーで製品アイコンをクリックします。

既定では、この製品アイコンは、メニューバーに常時表示されます。メニューバーの製品アイコンは非表示にすることもできます。

[メニューバーでのアイコンの非表示](#)

1. メニューバーで製品アイコンをクリックし、**[設定]** を選択します。
本製品の設定ウィンドウが表示されます。
2. **[インターフェイス]** タブの **[製品アイコン]** セクションで、**[メニューバーに表示する]** をオフにします。

本製品のウィンドウを開くと、製品アイコンは **Dock** にも表示されます。

製品アイコンのメニューからメインウィンドウにアクセスして、次の操作を実行できます：

- 保護機能を無効にする。
- 保護機能を有効にする。
- プロテクションセンターを開く。
- 簡易スキャンを開始する。
- アップデートを実行する。
- 本製品の設定ウィンドウを開く。
- Kaspersky Endpoint Security を終了する。

本製品の設定ウィンドウ

[本製品の設定ウィンドウを開く](#)

次のいずれかを実行します：

- メニューバーで製品アイコンをクリックし、**[設定]** を選択します。
- メニューバーで、**[Kaspersky Endpoint Security]** → **[設定]** の順にクリックします。

- 本製品が実行されている場合、**Dock**にある本製品のアイコンをクリックし、**〔設定〕**を選択します。

設定ウィンドウにある次のタブを使用して、アプリケーションの設定に簡単にアクセスできます：

- **脅威対策**：このタブで、コンピュータの保護を有効または無効にしたり、ファイル脅威対策、ウェブ脅威対策、ネットワーク脅威対策を設定したりできます。
- **スキャン**：このタブで、スキャンタスクの設定とスキャンタスクの開始スケジュールを設定します。
- **脅威**：このタブで、検知するオブジェクトのカテゴリの選択、信頼ゾーンの作成、バックアップの設定の指定が可能です。
- **詳細**：Kaspersky Security Network へ参加するかどうかを選択します。
- **アップデート**：このタブで、本製品のアップデート設定の指定、定義データベースの以前のバージョンへのロールバックが可能です。
- **インターフェイス**：このタブで、レポート、隔離、バックアップの設定を指定したり、トレースファイルへのデバッグ情報の記録を有効または無効にすることができます。

 を使用すると、管理者権限を持たないユーザが Kaspersky Endpoint Security の設定を編集できないようにすることができます。このボタンは、本製品の設定ウィンドウの下部にあります。設定を編集するには、管理者の資格情報を入力してください。

 をクリックすると、現在のウィンドウのすべての設定の説明が記載された Kaspersky Endpoint Security のヘルプが表示されます。現在アクティブなウィンドウについてのヘルプは、**〔ヘルプ〕**メニューから **〔このウィンドウのヘルプを開く〕**を選択して表示することもできます。

通知について

Kaspersky Endpoint Security は、通知を表示して製品のイベントを知らせます。通知は、コンピュータのオペレーティングシステムのバージョンによっては、オペレーティングシステムの通知センターに表示されます。通知の外見は、オペレーティングシステムの通知設定で設定されているオプションによって異なります。

イベントは、その重要性に応じて次の 3 つの種別に分類されます：

- **緊急**：コンピュータのセキュリティにとって重大な脅威になるイベント（悪意のあるオブジェクト、脆弱性、Kaspersky Endpoint Security の問題の検知）。緊急イベントにはすぐに対応する必要があります。緊急イベントについての通知は無効にしないでください。
- **重要**：早急な対応は必要ないが、今後、コンピュータのセキュリティにとって脅威になる可能性のあるイベント。
- **情報**：情報のために報告されるイベント。

通知の無効化

1. メニューバーで製品アイコンをクリックし、**〔設定〕**を選択します。
本製品の設定ウィンドウが表示されます。
2. **〔インターフェイス〕** タブの **〔通知〕** セクションで、**〔通知を有効にする〕** をオフにします。

緊急イベント以外の記録を有効にする

1. メニューバーで製品アイコンをクリックし、**〔設定〕**を選択します。
本製品の設定ウィンドウが表示されます。
2. **〔インターフェイス〕** タブの **〔レポート〕** セクションで、**〔緊急イベント以外も記録する〕** をオンにして、本製品の情報に関する通知を受信します。

通知が有効が無効にかかわらず、**製品のレポート**には、Kaspersky Endpoint Security の動作中に発生したイベントに関する情報が記録されます。

通知では音が鳴ることもあります（たとえば、マルウェア検知の通知など）。通知音を無効にすることができます。

緊急イベント以外のイベントを記録すると、レポートファイルのサイズが非常に大きくなります。この設定は、ファイル脅威対策にのみ適用されることにご注意ください。

通知音を無効にする

1. メニューバーで製品アイコンをクリックし、**〔設定〕**を選択します。

本製品の設定ウィンドウが表示されます。

2. [インターフェイス] タブの [通知] セクションで、[マルウェアの検知時に警告音を鳴らす] をオフにします。

イベントに対して操作が必要な場合、通知ウィンドウが表示されます。たとえば、悪意のあるオブジェクトが検知された場合、そのオブジェクトを削除するか駆除するかを選択するメッセージが表示されます。通知ウィンドウは、処理を選択するまで表示されます。

Kaspersky Endpoint Security のライセンス

使用許諾契約書について

使用許諾契約書は、ユーザと AO Kaspersky Lab との間で交わされる契約であり、製品の使用条件が定められています。

重要：製品を使い始める前に、使用許諾契約書をよく読んでください。

使用許諾契約書の条項は、次の方法で確認することができます：

- Kaspersky Endpoint Security のインストール時
- 製品のインストールフォルダの `license.txt` を読む

Kaspersky Endpoint Security をインストールすることで、使用許諾契約書の条項について理解し同意したことになります。使用許諾契約書の条項に同意しない場合は、Kaspersky Endpoint Security のインストールをキャンセルし、製品を使用しないでください。

ライセンスについて

ライセンスは、署名付きのライセンス契約（使用許諾契約書）に基づいて提供される、Kaspersky Endpoint Security を使用する期限付きの権利です。

サービスの範囲と有効期間は、本製品のアクティベーションに使用されるライセンスの種別によって異なります。

次のライセンス種別があります：

- **試用版**
製品の試用を目的とした無償ライセンス。試用版ライセンスは通常、有効期間が短く設定されています。
試用版ライセンスの有効期限が切れると、すべての Kaspersky Endpoint Security 機能が無効になります。本製品を引き続き使用するには、製品版ライセンスを購入する必要があります。
試用版ライセンスでアプリケーションを使用できるのは、1回の試用期間のみです。
- **製品版**
有料ライセンス。
製品版ライセンスの有効期限が切れると、本製品の主要な機能が無効になります。Kaspersky Endpoint Security を引き続き使用する場合は、製品版ライセンスを更新してください。製品版ライセンスの有効期限が切れると、本製品を引き続き使用できなくなり、デバイスから削除する必要があります。
有効期間の終了前にライセンスを更新し、すべてのセキュリティ脅威からの最大限の保護が中断されることなく確保できるようにしてください。

定額制サービスについて

Kaspersky Endpoint Security の定額制サービスは、特定のパラメータ（有効期間終了日、保護対象のデバイスの台数）を持つ購入注文です。Kaspersky Endpoint Security の定額制サービスは、サービスプロバイダー（ご利用の ISP など）から注文できます。定額制サービスは、サービスプロバイダーの Web サイトの加入者用ページで管理できます。定額制サービスの更新やキャンセル、期間の短縮、保護対象のデバイスの台数の変更などが可能です。

定額制サービスには、有効期限あり（1年など）と無期限（有効期限なし）があります。有効期限付きの定額制サービスの期間終了後に Kaspersky Endpoint Security を引き続き利用する場合は、手動で更新する必要があります。有効期限がない定額制サービスの場合、サービスプロバイダーに料金を支払い続けている限り、自動で更新されます。

有効期限付きの定額制サービスを利用している場合、有効期間が終了すると、サービスを更新するための猶予期間が付与されます。この猶予期間中は、本製品を引き続き使用できます。

定額制サービスのアップデートの期限、およびサービス更新の猶予期間の終了後も本製品を引き続き使用できますが、定義データベースがアップデートされなくなります。

定額制サービスのアップデートと保護の期限、およびサービス更新の猶予期間の終了後、本製品はコンピュータの保護を停止します。

定額制サービスを利用するには、サービスプロバイダーから提供されたアクティベーションコードを追加する必要があります。定額制サービスを利用している場合、別のアクティベーションコードを使用して定額制サービスを更新することはできません。定額制サービスの有効期間の終了後か、定額制サービスをキャンセルした場合に限り、別のアクティベーションコードを適用できます。定額制サービスをキャンセルするには、**Kaspersky Endpoint Security** を購入したサービスプロバイダーまでご連絡ください。

注意：別のアクティベーションコードは、現在のライセンスが削除されないと適用できません。定額制サービスにはライセンス情報ファイルは含まれていません。定額制サービスは予備のライセンスとして追加できません。予備のライセンスは、定額制サービスの使用時には追加できません。

既に有効なライセンスで **Kaspersky Endpoint Security** を使用していて定額制サービスに切り替えたい場合は、現在のライセンスを削除してください。その後、定額制サービスのライセンスで本製品をアクティベートできます。このコンピュータで本製品のアクティベートに以前使用していたアクティベーションコードは、別のコンピュータで使用できます。

注意：利用可能な定額制サービスのオプションは、サービスプロバイダーによって異なる場合があります。サービスプロバイダーによっては、定額制サービスを更新する際の猶予期間がない場合があります。

ライセンス証明書について

ライセンス証明書とは、ライセンス情報ファイルまたはアクティベーションコードに付随して受け取る文書です。

ライセンス証明書には、提供されたライセンスに関する次の情報が含まれています：

- ライセンス情報またはオーダー番号
- ライセンスが適用されるユーザの情報
- 提供されたライセンスを使用したアクティベーションが可能である製品の情報
- ライセンスの上限（提供されたライセンスで使用可能な製品が使用できるデバイスの台数など）
- ライセンスの有効期間の開始日
- ライセンスの有効期間または有効期間の終了日
- ライセンス種別

ライセンス情報について

ライセンス情報とは、使用許諾契約書の条項に基づいてアクティベーションを適用して製品を使用できる数値の並びです。ライセンス情報は、カスペルスキーによって生成されます。

製品にライセンス情報を追加するには、ライセンス情報ファイルを適用するか、アクティベーションコードを入力します。ライセンス情報は、製品に追加した後、インターフェイスに一意の英数字の並びで表示されます。

使用許諾契約書の条項に違反した場合、カスペルスキーがライセンス情報をブロックします。ライセンス情報がブロックされた際に、製品を使用したい場合は、別のライセンス情報を追加する必要があります。

ライセンスには、現在のライセンスと予備のライセンスがあります。

現在のライセンスは、現在製品で使用されているライセンスです。現在のライセンスは、試用版ライセンス、製品版ライセンス、定額制サービスのいずれかを追加できます。現在のライセンスに指定できるのは1つだけです。

予備のライセンスは、現在使用されていない、製品の使用ライセンスです。現在のライセンスの有効期間が終了すると、予備のライセンスが自動的に現在のライセンスになります。予備のライセンスは、現在のライセンスが追加されていないと追加できません。

試用版ライセンスは現在のライセンスとして追加することができます。試用版ライセンスを予備のライセンスとして追加することはできません。試用版ライセンスが有効な場合、予備のライセンスを追加することはできません。

アクティベーションコードについて

アクティベーションコードは、一意の 20 文字の半角英数字です。 **Kaspersky Endpoint Security** をアクティベートするライセンス情報を追加するには、アクティベーションコードを入力する必要があります。アクティベーションコードは、**Kaspersky Endpoint Security** を購入した時、または **Kaspersky Endpoint Security** の試用版をリクエストした時に指定したメールアドレスに送られます。

アクティベーションコードを使用して本製品をアクティベートするには、カスペルスキーのアクティベーションサーバに接続するためにインターネット接続が必要です。

アクティベーション後にアクティベーションコードを紛失した場合は、カスペルスキーのテクニカルサポートにご連絡ください。

ライセンス情報ファイルについて

ライセンス情報ファイルは、カスペルスキーにより提供される、拡張子 .key を持つファイルです。ライセンス情報ファイルを追加することで本製品のアクティベーションが実行されるよう設計されています。

Kaspersky Endpoint Security の購入時または試用版の Kaspersky Security の注文時に登録したメールアドレスで、ライセンス情報ファイルを受け取ります。

ライセンス情報ファイルを使って本製品のアクティベーションを実行するために、カスペルスキーのアクティベーションサーバに接続する必要はありません。

誤ってライセンス情報ファイルを削除してしまった場合は、復元することができます。カスペルスキーカンパニーアカウントを登録する際に、ライセンス情報ファイルが必要になる場合があります。

ライセンス情報ファイルを復元する方法は、次のいずれかです：

- ご購入元の販売代理店へ問い合わせる
- [カスペルスキーの Web サイト](#) で、使用可能なアクティベーションコードを使用してライセンス情報ファイルを取得する

データ提供について

使用許諾契約書

Kaspersky Endpoint Security をアクティベーションコードでアクティベートする場合、カスペルスキー製品が合法的に使用されていることを確認し、配信と使用に関する統計情報を提供するため、Kaspersky Endpoint Security の使用時に次の情報を自動的に提供することに同意したことになります：

- インストールされた本ソフトウェアの種別、バージョンおよび言語。
- インストールされたアップデートのバージョン。
- 端末の識別子、およびこの端末への本ソフトウェアのインストールの識別子。
- アクティベーションコードと使用中のライセンスの一意なアクティベーション識別子。
- オペレーティングシステムの種別、バージョンおよびビット数。
- 本ソフトウェアが仮想環境上にインストールされている場合はその仮想環境の名前。
- 情報が提供された時に動作中の本ソフトウェア機能の識別子。
- サポートされているデータソース。
- タイムアウト。
- ユーザのコンピュータの日付と時刻。
- プロトコルバージョン。
- プロトコルコンテンツ種別。
- プロトコルコンテンツの長さ。
- 使用されるデータ圧縮の種別。
- アクティベーションチケットの署名の種別。
- 地域のアクティベーションセンターの識別子。
- SHA1 アルゴリズムを使用して計算されたアクティベーションコードハッシュ。
- SHA1 アルゴリズムを使用して計算されたチケット本体ハッシュ。
- ライセンスチケットの作成日時。
- ライセンスアクティベーションの識別子。
- 現在のライセンスチケットの識別子。
- ライセンスチケットシーケンスの識別子。
- ライセンスアクティベーションの日付と時刻。
- ライセンス終了の日付と時刻。

- ライセンスのステータス。
- ライセンスのバージョン。
- ユーザのコンピュータの一意な識別子。
- ライセンスチケットヘッダーのバージョン。
- アプリケーションの名前。
- 転送されたデータ種別。
- 転送されたデータのスキームバージョン。
- オペレーティングシステムの詳細バージョン。
- 使用されている仮想マシンの記述。
- 互換性のあるアプリケーションの ID リスト。

カスペルスキーのアップデートサーバを使用してアップデートをダウンロードする場合、アップデート手続きの効率化を図る目的で、データベースやモジュールのアップデートの際のアプリケーション識別のため、次の情報を定期的に提供することに同意します：

- ソフトウェア ID (ApplID)。
- 現在のライセンスの識別子。
- ソフトウェアインストールの一意の識別子 (InstallationID)。
- アップデートタスク起動の一意の識別子 (SessionID)。
- ソフトウェアのバージョン (BuildInfo)。

Kaspersky Security Network (KSN) に関する声明

KSNを使用すると、情報やネットワークセキュリティの脅威に対するソフトウェアの反応速度が向上する場合があります。前述の目的は次の項目により実現します：

- スキャン対象のオブジェクトの評価の決定。
- 検知の回避策が複雑化した情報セキュリティ上の未知の脅威やその発生源の識別。
- 速やかに適切な手段を講じることで、ユーザのコンピュータ上で保存および処理されるデータの保護レベルの向上。
- 誤検知の可能性の減少。
- 本ソフトウェアの機能の効率の向上。
- ユーザのコンピュータの感染に関する調査。
- カスペルスキー製品のパフォーマンス向上。
- 既知のオブジェクトの評価や検知件数についての参照情報の受信。
- 本ソフトウェアのインストール、アンインストール、アップデートに関連するエラーの迅速な検出および修正。

KSN の使用中に、カスペルスキーはデータを自動的に受信し処理します：ユーザにより送信されるデータは、インストールされたライセンスの種類および Kaspersky Security Network の使用設定により異なります。

1〜4 ノード用のライセンスを使用している場合、権利者は Kaspersky Security Network の使用中に次のデータを自動的に受け取り処理します。

- 適用されているライセンスの情報：ライセンスの種類および有効期間、ライセンスの有効期限までの日数、ライセンスの購入元である代理店の識別子、地域のアクティベーションセンターの識別子、アクティベーションコードのチェックサム、SHA1 アルゴリズムを使用して計算されたチケットボディのハッシュ、ライセンスチケットの作成日時、ライセンス情報の識別子、ライセンスチケットの識別子、ライセンスチケットのシーケンスの識別子、ユーザのコンピュータの一意な識別子、ライセンスチケットが有効になった日付、ライセンスチケットの有効期限、ライセンスチケットの現在のステータス、チケットヘッダーのバージョン、ライセンスのバージョン、チケットヘッダーの署名に使用された証明書識別子、ライセンスファイルのチェックサム、チケットヘッダーの署名元のシリアル番号、認証トークン。
- インストールされた本ソフトウェアの詳細バージョン。インストールされた本ソフトウェアの種別。ソフトウェアアップデートの ID。評価サービスの ID。プロトコルタイプの ID。地域のアクティベーションセンターの ID。本ソフトウェアのサービスの決定のうち取り消されたもののリストのバージョン。トリガーされた本ソフトウェアの定義データベースのレコードの ID。トリガーされた本ソフトウェアの定義データベースのレコードのタイムスタンプ。トリガーされた本ソフトウェアの定義データベースのレコードの種別。本ソフトウェアのコンピュータへのインストールのインスタンスの一意な ID。ライセンスがアクティベートされた日付。ライセンスの有効期限日。ライセンスの識別子。本ソフトウェアが使用中のライセンスのステータス。処理中のオブジェクトのチェックサム種別。検知されたマルウェアの名前、ユーザのコンピュータまたはデータに損害を与える目的で使用される可能性がある正規のソフトウェアの名前。処理中のオブジェクトのチェックサム。本ソ

ソフトウェアのアクティベーションコードのチェックサム。本ソフトウェアの詳細バージョン。一意のデバイス ID。本ソフトウェアの ID。本ソフトウェアのライセンス情報ファイルのチェックサム。本ソフトウェアのライセンスの提供に使用された情報形式の ID。本ソフトウェアのライセンスチケットのヘッダーへの署名に使用される証明書の識別子。本ソフトウェアのライセンスチケットの作成日時。本ソフトウェアのライセンスチケットのチェックサム。本ソフトウェアのライセンスチケットのバージョン。本ソフトウェアのアクティベーションコードのバージョン。権利者のインフラストラクチャへのリクエストに含まれるデータの形式。使用中のライセンスチケットの ID。本ソフトウェアのコンポーネントの ID。本ソフトウェアの動作の結果。エラーコード。アクセスされた Web サービスのアドレス (URL、IP)。ポート番号。Web サービスのリクエスト元の URL (リファラー)。証明書の公開鍵。スキャンされたオブジェクトのデジタル証明書のサムプリントとハッシュアルゴリズム。

5 ノード以上用のライセンスを使用している場合、カスペルスキーは Kaspersky Security Network の使用中に次のデータを自動的に受け取り処理します：

- コンピュータにインストールされているオペレーティングシステム (OS) やサービスパックのバージョンに関する情報、OS カーネルファイルのバージョンおよびチェックサム (MD5、SHA2-256、SHA1)、OS 実行モードの識別子。OS のバージョン、OS のビルド番号、OS のアップデート番号、OS のエディション、OS のエディションに関する詳細情報。OS のサービスパックのバージョン OS の起動日時。ふるまい分析のサブシステムにおける OS 動作に関するイベントの処理遅延時間。現在の種別の遅延された OS 動作イベントの数。プロアクティブディフェンスのサブシステムにおける OS 動作に関するイベントの処理遅延時間。処理された OS 動作イベントの数。処理された OS 同期動作イベントの数。現在の種別のすべての OS 動作イベントの合計遅延時間。持続的イベントを記憶するサブシステムにおける、OS 動作に関するイベントの処理遅延時間。すべての OS 動作イベントの合計遅延。待機中の OS 同期動作イベントの数。OS 内の動作イベントを受信した日時。
- 以前、OS の再起動が失敗した履歴：再起動に失敗した回数。
- インストールされている本製品に関する情報およびアンチウイルス保護状況：ソフトウェアのインストール識別子 (PCID) 本ソフトウェアの定義データベースのレコードのバージョン、コンピューター上にインストールされたアプリケーションのインスタンスの一意な識別子、アプリケーションの種別、アプリケーション種別の識別子、インストールされたアプリケーションの詳細バージョン、アプリケーションの設定のバージョンの識別子、コンピューター種別の識別子、アプリケーションがインストールされたコンピューターの一意な識別子、権利者のサービスにおける一意なユーザー識別子、言語および動作状況、インストールされたソフトウェアコンポーネントのバージョンと動作状況、権利者のサービスに接続するために使用されたプロトコルのバージョン、インストールされた本ソフトウェアの詳細バージョン。インストールされた本ソフトウェアの種別。ソフトウェアアップデートの ID。評価サービスの ID。プロトコルタイプの ID。地域のアクティベーションセンターの ID。本ソフトウェアのサービスの決定のうち取り消されたもののリストのバージョン。トリガーされた本ソフトウェアの定義データベースのレコードの ID。トリガーされた本ソフトウェアの定義データベースのレコードのタイムスタンプ。トリガーされた本ソフトウェアの定義データベースのレコードの種別。本ソフトウェアのコンピューターへのインストールのインスタンスの一意な ID。ライセンスがアクティベートされた日付。ライセンスの有効期限。ライセンスの識別子。本ソフトウェアが使用中のライセンスのステータス。処理中のオブジェクトのチェックサム種別。検知されたマルウェアの名前、ユーザのコンピューターまたはデータに損害を与える目的で使用される可能性がある正規のソフトウェアの名前。処理中のオブジェクトのチェックサム。本ソフトウェアのアクティベーションコードのチェックサム。本ソフトウェアの詳細バージョン。本ソフトウェアの ID。本ソフトウェアのライセンス情報ファイルのチェックサム。本ソフトウェアのライセンスの提供に使用された情報形式の ID。本ソフトウェアのライセンスチケットのヘッダーへの署名に使用される証明書の識別子。本ソフトウェアのライセンスチケットの作成日時。本ソフトウェアのライセンスチケットのチェックサム。本ソフトウェアのライセンスチケットのバージョン。本ソフトウェアのアクティベーションコードのバージョン。権利者のインフラストラクチャへのリクエストに含まれるデータの形式。使用中のライセンスチケットの ID。本ソフトウェアのコンポーネントの ID。本ソフトウェアの動作の結果。エラーコード。アクセスされた Web サービスのアドレス (URL、IP)。ポート番号。Web サービスのリクエスト元の URL (リファラー)。定義データベースのアップデートと適用のサイクル数。定義データベースが最後にアップデートおよび適用された日時。本ソフトウェアの定義データベースの公開日時。本ソフトウェアのコンポーネントのバージョン。ソフトウェアアップデートの ID。インストールされた本ソフトウェアの種別。システムウォッチャーの開始日時。本ソフトウェアのインストール日時。システムウォッチャーによって統計が送信される確率。システムウォッチャーによる標準処理時間よりも長い時間がかかったイベントのコード。システムウォッチャーによる標準処理時間を超えたイベントのデータベース処理時間。システムウォッチャーによるイベントの処理に許可される最大時間。システムウォッチャーによる標準処理時間を超えたイベントの処理時間。システムウォッチャーによる標準処理時間よりも長い時間がかかったイベントの総数。
- 処理したすべてのオブジェクトおよび操作に関する情報：処理中のオブジェクトに対する本ソフトウェアの判定、ディレクトリコード、処理中のオブジェクトのサイズ、処理中のオブジェクトのチェックサム (SHA256)、システムウォッチャーを使用して検知されたソフトウェアの数、システムウォッチャーでソフトウェアを検知した日時、検知の特性、トリガーされた本ソフトウェアの定義データベースのレコードの ID。システムウォッチャーでソフトウェアを検知した理由、処理中のオブジェクトのチェックサム (MD5)、モジュールの整合性チェックの結果、処理中のオブジェクトの名前、トリガーされた本ソフトウェアの定義データベースのレコードの種別、処理中のオブジェクトへのパス。スキャンしたオブジェクトの製造元の名前、スキャンの日時、URL およびダウンロードされたリファラーのアドレス、スキャンされたファイルのサイズおよびパス、アーカイブかどうかのフラグ、ファイルの作成日時、圧縮されていた場合はバックアーカイブの名前、サイズおよびチェックサム (MD5、SHA2-256)、ファイルのエントロピー、ファイルの種別、ファイル種別コード、ファイルが実行可能かどうかのフラグ、識別子および形式、オブジェクトのチェックサム (MD5、SHA2-256)、オブジェクトの追加チェックサムの種別および値、オブジェクトのデジタル署名 (証明書) に関するデータ：証明書の発行元に関する情報、前回の統計が送信されてからオブジェクトが実行された回数、本製品のスキニングタスクの識別子、オブジェクトの評価に関する情報の受信手段、TARGET フィルターの値、適用可能な検知技術の技術的パラメータ。処理中のオブジェクトへのパス。ディレクトリコード。
- 実行ファイルの場合：ファイルセクションの情報量、評価の検証フラグまたはファイルの署名フラグ、検証対象のオブジェクトに読み込まれたアプリケーションの名前、種別、ID 種別、チェックサム (MD5) およびサイズ、アプリケーションのパスおよびテンプレートのパス、自動実行リストの署名、エントリの日時、属性のリスト、圧縮ソフトウェアの名前、アプリケーションのデジタル署名に関する情報：発行者の証明書、アップロードされたファイルの MIME 形式での名前、ファイルが作成された日時。
- 実行中のアプリケーションおよびそのモジュールに関する情報：実行中のファイルのチェックサム (MD5、SHA2-256)、ファイルのサイズ、属性、作成日時、圧縮ソフトウェアの名前 (ファイルが圧縮されている場合)、ファイル名、システム上で実行されているプロセスに関する情報 (プロセス ID (PID)、プロセス名、プロセスを開始したアカウントに関する情報、プロセスを開始したアプリケーションおよびコマンド、プロセスのファイルへの完全パスおよび開始したコマンドライン、プロセスが属するアプリケーションの説明 (アプリケーション名および配信元の情報)、使用されるデジタル証明書およびそれらの正当性を検証するために必要な情報またはファイルのデジタル署名が存在しない旨のフラグ)、プロセスに読み込まれたモジュールの情報：名前、サイズ、種別、作成日、属性、チェックサム (MD5、SHA2-256、SHA1) およびパス、PE ファイルのヘッダー情報、圧縮ソフトウェア名 (ファイルが圧縮されている場合)、統計情報の有効性および使用可否に関する情報、送信される統計情報の生成条件の識別子。
- 脅威または脆弱性が検知された場合、検知されたオブジェクトに関する情報に加え、次の情報が提供されます：定義データベース中のレコードの識別子、バージョンおよび種別、カスペルスキーの分類による脅威名、定義データベースの最終アップデート日時、実行ファイルの名前、

脅威が検知された URL をリクエストしたアプリケーションのファイルのチェックサム (MD5)、検知した脅威の IP アドレス (IPv4 または IPv6)、脆弱性の識別子および脅威レベル、脅威を検知した Web ページの URL およびリファラー。

- 悪意のある可能性があるオブジェクトが検知された場合、プロセスのメモリ内のデータに関する情報が提供されます。
- ネットワーク攻撃の情報：攻撃元コンピュータの IP アドレスおよびユーザのコンピュータ上でネットワーク攻撃の標的にされたポート番号、攻撃プロトコルの ID、名前および攻撃種別。
- ネットワーク接続に関する情報：ポートを開いたプロセスを起動したファイルのバージョンおよびチェックサム (MD5、SHA2-256、SHA1)、プロセスのファイルのパスおよびデジタル署名、ローカルおよびリモートの IP アドレス、ローカルおよびリモート接続のポート番号、接続状況、ポートが開かれた時刻。
- 危険なオブジェクトまたは疑わしいオブジェクトを検知した Web ページの URL および IP アドレス、この URL をリクエストしたファイルの名前、サイズおよびチェックサム、識別子、検知結果の決定基準に使用されたルールの重み係数および度数、攻撃の目的に関する情報。
- インストール済み本ソフトウェアおよび定義データベースのアップデートに関する情報：アップデートタスクの完了状況、アップデート中に発生した可能性のあるエラーの種別、失敗したアップデートの数、アップデートを実行した本ソフトウェア機能の識別子。
- Kaspersky Security Network (KSN) の使用に関する情報：KSN の識別子、本ソフトウェアの識別子、本ソフトウェアの詳細バージョン、個人を特定できないようにしたお客様のデバイスの IP アドレス、KSN へのリクエストの実行品質を示す指数、KSN 用パケットの処理品質を示す指数、KSN へのリクエストの件数およびリクエストの種別に関する情報、統計情報の送信を開始した日時と終了した日時、KSN 設定のアップデートに関する情報：アクティブな設定の識別子、受信した設定の識別子、設定のアップデートのエラーコード。
- イベントに関するシステムログ内の情報：イベントのタイムスタンプ、イベントが検知されたログの名前、イベントの種別およびカテゴリ、イベントの発生源の名前およびイベントの説明。
- ファイルおよび URL の評価決定に関する情報：評価が要求された URL とその参照元、接続のプロトコルタイプ、アプリケーション種別の内部識別子、使用されているポートの番号、ユーザ識別子、スキャンされたファイルのチェックサム (MD5)、検知された脅威の種別、脅威の検知に使用したレコードに関する情報 (定義データベースのレコードの識別子、レコードのタイムスタンプと種別)。証明書の公開鍵。スキャンされたオブジェクトのデジタル証明書のサムプリントとハッシュアルゴリズム。
- 本ソフトウェアの地域分布に関する情報：本ソフトウェアのインストールおよびアクティベーションの日時、本ソフトウェアのアクティベーション用のライセンスを提供した代理店の識別子、本ソフトウェアの識別子、本ソフトウェアの言語版の識別子、本ソフトウェアに適用されたライセンスの識別番号、KSN に参加しているかどうかのフラグ。
- 適用されているライセンスの情報：ライセンスの種別および有効期間、ライセンスの有効期限までの日数、ライセンスの購入元である代理店の識別子、地域のアクティベーションセンターの識別子、アクティベーションコードのチェックサム、SHA1 アルゴリズムを使用して計算されたチケットボディのハッシュ、ライセンスチケットの作成日時、ライセンス情報の識別子、ライセンスチケットの識別子、ライセンスチケットのシーケンスの識別子、ユーザのコンピュータの一意な識別子、ライセンスチケットが有効になった日付、ライセンスチケットの有効期限、ライセンスチケットの現在のステータス、チケットヘッダーのバージョン、ライセンスのバージョン、チケットヘッダーの署名に使用された証明書の識別子、ライセンスファイルのチェックサム、チケットヘッダーの署名元のシリアル番号、認証トークン。
- コンピュータにインストールされているハードウェアに関する情報：搭載または接続された装置の種別、名前、機種名、ファームウェアのバージョン、パラメータ。
- 端末に関する情報：端末の識別子。
- ウェブコントロール機能の動作に関する情報：機能のバージョン、当該カテゴリに分類された理由および関連情報、分類された URL、ブロックまたは分類されたオブジェクトのホストの IP アドレス。

また、本ソフトウェアの提供する保護機能の効率性を向上させるため、権利者は、端末に損害を与え、情報セキュリティ上の脅威を作成する目的で侵入者に悪用される可能性のあるオブジェクトを受け取ることがあります。具体的なオブジェクトは次の通りです：

- 実行または非実行ファイルまたはその一部
- 端末の RAM の領域
- OS 起動時に採用されるセクタ
- ネットワーク通信のデータパケット
- 疑わしい、および悪意のあるオブジェクトを含む Web ページまたはメール
- WMI リポジトリ上のクラスおよびそれらのインスタンスの記述
- アプリケーション活動に関するレポート

アプリケーション活動に関するレポートには、ファイルおよびプロセスに関する次のデータが含まれます：

- 送信されるファイルの名前、サイズおよびバージョン、説明およびチェックサム (MD5、SHA2-256、SHA1)、ファイル形式の識別子、ファイルの製造元の名前、ファイルが属するアプリケーションの名前、端末上の完全パス、ファイルのパステンプレートコード、ファイルの作成日時および更新日時。
- 証明書の有効期間の開始日時と終了日時 (ファイルにデジタル署名がある場合)、署名適用の日時、証明書の発行者名、証明書の所有者に関する情報、証明書のフィンガープリント、公開鍵およびそれぞれの生成アルゴリズム、証明書のシリアル番号。

- プロセスを実行したアカウント名。
- プロセスが実行されている端末名のチェックサム（MD5、SHA2-256、SHA1）。
- プロセスウインドウのタイトル。
- 定義データベースの識別子、権利者の分類による検知された脅威の名前。
- 本製品で使用中のライセンスに関するデータ、識別子、種別および有効期限。
- 情報を提供した時の端末上のローカル時間。
- プロセスがアクセスしたファイルの名前とパス。
- プロセスがアクセスした URL と IP アドレス。
- 実行中のファイルをダウンロードした URL および IP アドレス。

また、誤検知を防ぐ目的で、権利者は信頼済みの実行または非実行ファイル、およびそれらの一部を受け取ることがあります。

[Kaspersky Security Network 声明を読む](#)

1. メニューバーで製品アイコンをクリックし、**〔設定〕** を選択します。
本製品の設定ウインドウが表示されます。
2. **〔詳細〕** タブで **〔KSN 声明を表示する〕** をクリックします。

トレースファイルには、次の情報が保存されます：

- 端末とオペレーティングシステムに関する情報（デバイスの一意な識別子、デバイスの種別、ネットワークデバイスの MAC アドレス、オペレーティングシステムの種別、オペレーティングシステムのバージョン）。
- 本製品および本製品のモジュールの動作に関する情報。
- 定額制サービスに関する情報（定額制サービスの種別、地域）。
- 言語、アプリケーションの識別子、アプリケーションのカスタマイズ、アプリケーションのバージョン、アプリケーションのインストールの一意な識別子、端末の一意な識別子に関する情報。
- マルウェア対策による端末の保護の状態、処理または検知されたすべてのオブジェクトおよびその対処（検知されたオブジェクトの名前、検知日時、ダウンロード元の URL、感染したファイルの名前とサイズ、それらのファイルのパス、攻撃元コンピュータの IP アドレスとネットワーク攻撃の標的になったポートの番号、マルウェアによる活動のリスト、望ましくない URL）、製品およびユーザによる関連する操作および決定。
- ユーザがダウンロードしたアプリケーションに関する情報（URL、属性、ファイルサイズ、ダウンロードプロセスに関する情報）。
- 起動したアプリケーションおよびそのモジュールに関する情報（サイズ、属性、作成日、PE ヘッダーの詳細、地域、製品名、場所、パッケージ）。
- インストールされているカスペルスキー製品のインターフェイスのエラーや使用に関する情報。
- ネットワーク接続に関する情報：リモートコンピュータおよびユーザのコンピュータの IP アドレス、接続に使用されたポート番号、接続のネットワークプロトコル。
- IT および通信ネットワークを介してコンピュータから送受信されたネットワークパケットに関する情報。
- 送受信されたメールおよびインスタントメッセージに関する情報。
- アクセスされた URL に関する情報：オープンなプロトコルを使用して接続が確立された時間、Web サイトのログインおよびパスワードに関する情報、Cookie の内容。
- サーバの公開証明書。

トレースファイルには、本製品の修正に必要な情報のみが含まれます。カスペルスキーは、Kaspersky Endpoint Security の動作中に発生したエラーと関係があるインシデントを調査するため、トレースファイルを使用します。

既定では、トレースファイルの作成は無効になっています。トレースファイルの作成は、本製品の設定で有効にできます。

トレースファイルのカスペルスキーへの送信は、手動でのみ可能です。本製品が自動的にトレースファイルをカスペルスキーに送信することはありません。

トレースファイルのカスペルスキーへの送信方法を選択できます。

カスペルスキーへトレースファイルを送信する前に、含まれるデータを確認してください。

重要：トレースファイルには、個人情報または機密情報が含まれる可能性があります。カスペルスキーへトレースファイルを送信することで、送信したトレースファイル内のすべての情報をカスペルスキーに提供することに同意し、送信時に使用された方法にも同意したことになります。

コンピュータまたはデータに損害を与えるために悪用された可能性があるファイルやファイルの一部も、解析のために追加でカスペルスキーに提供されることがあります。

カスペルスキーは、このようにして受け取ったすべての情報を法律および適用可能なカスペルスキーの内規に基づいて保護します。データはセキュアな通信で転送されます。

Kaspersky Security Network への参加は任意です。参加するかどうかは、Kaspersky Endpoint Security のインストール時に決定します。ただし、インストール後にいつでも変更できます。

Kaspersky Endpoint Security のアクティベーション

重要：Kaspersky Endpoint Security をアクティベートする前に、コンピュータの現在の日時が実際の日時と一致していることを確認してください。

アクティベーションの実行では、本製品にライセンスを追加します。Managed Detection and Response コンポーネントは、個別に有効化します。このコンポーネントを使用するには、[Kaspersky Managed Detection and Response](#) を、[Kaspersky Security Center 管理コンソール](#)または [Web コンソール](#)で有効化する必要があります。

Endpoint Detection and Response コンポーネントが現在のライセンスでサポートされていない場合は、Kaspersky Endpoint Detection and Response を個別にアクティベートする必要があります。

注意：本製品をアクティベートするには、インターネット接続が必要です。

[試用版をアクティベートする](#)

1. 本製品のメインウィンドウを開きます。
2. 本製品のメインウィンドウのサイドバーで、**［ライセンス］** をクリックします。
［ライセンス］ ウィンドウが開きます。
3. **［ライセンス］** ウィンドウの **［アクティベート］** をクリックします。
Kaspersky Endpoint Security がカスペルスキーのアクティベーションサーバに接続し、データを送信して検証します。データの検証に成功すると、無料の試用版のライセンスが製品に送信され、追加されます。

重要：Kaspersky Endpoint Security の試用版は、このコンピュータで以前に一度も本製品がアクティベートされていない場合に限りアクティベートできます。

[アクティベーションコードで本製品をアクティベートする](#)

1. 本製品のメインウィンドウを開きます。
2. 本製品のメインウィンドウのサイドバーで、**［ライセンス］** をクリックします。
［ライセンス］ ウィンドウが開きます。
3. **［ライセンス］** ウィンドウで、Kaspersky Endpoint Security の購入時に取得したアクティベーションコードを入力します。
4. **［アクティベート］** をクリックします。

注意：アクティベーションコードは、xxxxx-xxxxx-xxxxx-xxxxx の形式で表される、一意の 20 文字の半角英数字です。

本製品がカスペルスキーのアクティベーションサーバに接続し、入力されたアクティベーションコードを送信して信頼性を検証します。アクティベーションコードが正常に検証されたら、自動的にライセンス情報が提供されて、追加されます。

注意：取得したアクティベーションコードによっては、登録フォームに入力する必要がある場合があります。

アクティベーションコードの検証に失敗した場合、それに応じた通知が表示されます。この場合は、テクニカルサポートまでご連絡ください。

アクティベーションコードでのアクティベートが完了すると、次の情報が **「ライセンス」** ウィンドウに表示されます：

- ライセンスまたは定額制サービスのステータス
- 現在のライセンス
- 予備のライセンス（ある場合）
- ライセンス種別と、現在のライセンスまたはサブスクリプションで本製品を使用できるコンピュータの数
- 現在のライセンスまたはサブスクリプションで使用可能なアプリケーションの機能
- 有効期間終了日時
- ライセンスの有効期間終了までの残りの日数

ライセンス情報を表示する

[ライセンス情報を表示する](#)

1. 本製品のメインウィンドウを開きます。
 2. 本製品のメインウィンドウのサイドバーで、 **「ライセンス」** をクリックします。
- 「ライセンス」** ウィンドウが開きます。

「ライセンス」 ウィンドウには、次の情報が表示される場合があります：

- ライセンスまたは定額制サービスのステータス
- 現在のライセンス
- 予備のライセンス（ある場合）
- ライセンス種別と、現在のライセンスまたはサブスクリプションで本製品を使用できるコンピュータの数
- 現在のライセンスまたはサブスクリプションで使用可能なアプリケーションの機能
- 有効期間終了日時
- ライセンスの有効期間終了までの残りの日数

ライセンスと定額制サービスの管理

現在のライセンスの有効期間が終了し、適用されている予備のライセンスがない場合、ライセンスを更新する必要があります。ライセンスの有効期間が終了すると、製品は引き続き動作しますが、機能が制限されます（アップデート、**Kaspersky Security Network**、**Kaspersky Security Center** による **FileVault** ディスク暗号化が使用できなくなります）。引き続きすべてのコンポーネントを使用でき、マルウェアスキャンも実行できますが、使用される定義データベースは、ライセンスの有効期間終了までにインストールされたものに限られます。

重要：アップデートされていない定義データベースを使用している場合、コンピュータが感染するリスクが高くなります。

[ライセンスを更新する](#)

1. 本製品の [メインウィンドウ](#) のサイドバーで、 **「プロテクションセンター」** をクリックします。
- 「プロテクションセンター」** ウィンドウが表示されます。

2. [プロテクションセンター] ウィンドウで、[更新] をクリックします。

ライセンス更新に関する情報が掲載された Web ページが表示されます。オンラインストアからライセンスを更新した場合、決済完了後に、フォームに入力したメールアドレス宛てに Kaspersky Endpoint Security のアクティベーションコードが送信されます。

定額制サービスの利用中は、定額制サービスの有効期間が終了するまで、Kaspersky Endpoint Security が定期的にアクティベーションサーバに自動接続します。

有効期限のない定額制サービスを利用している場合、定額制サービスは自動で更新されます。

有効期限付きの定額制サービスで本製品を使用している場合、定額制サービスを更新するための猶予期間が終了すると、通知が表示され、定額制サービスの自動更新と定義データベースのアップデートが停止します。

この場合、Kaspersky Endpoint Security の購入元に連絡して手動で定額制サービスを更新できます。

[定額制サービスを更新する](#)

1. 本製品のメインウィンドウを開きます。
2. 本製品のメインウィンドウのサイドバーで、[ライセンス] をクリックします。
[ライセンス] ウィンドウが開きます。
3. [ライセンス] ウィンドウで、[サービスプロバイダーの Web サイトにアクセス] をクリックします。
サービスプロバイダーの Web サイトが開きます。

ご利用の定額制サービスの契約状態は古くなる場合があります。この場合、手動で定額制サービスの契約状態を更新する必要があります。定額制サービスが最新のものでない場合、定義データベースのアップデートを停止するか（アップデート用定額制サービスの場合）、コンピュータの保護およびスキャンタスクの実行を停止します（アップデートと保護用の定額制サービスの場合）。

[定額制サービスの契約状態を更新する](#)

1. 本製品のメインウィンドウを開きます。
2. 本製品のメインウィンドウのサイドバーで、[ライセンス] をクリックします。
[ライセンス] ウィンドウが開きます。
3. [ライセンス] ウィンドウで、 をクリックします。

ワークステーションのライセンス種別に応じた製品機能の比較

ワークステーション向けの Kaspersky Endpoint Security で利用できる機能の組み合わせはライセンス種別により異なります（下の表を参照）。

Kaspersky Endpoint Security 機能の比較

機能	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert
先進の脅威対策						
Kaspersky Security Network	✓	✓	✓	✓	✓	✓
ふるまい検知	✓	✓	✓	✓	✓	✓
脆弱性攻撃ブロック	✓	✓	✓	✓	✓	✓
修復エンジン	✓	✓	✓	✓	✓	✓
脅威対策						
ファイル脅威対策	✓	✓	✓	✓	✓	✓
ウェブ脅威対策	✓	✓	✓	✓	✓	✓
メール脅威対策	✓	✓	✓	✓	✓	✓
ファイアウォール	✓	✓	✓	✓	✓	✓

ネットワーク脅威対策	✓	✓	✓	✓	✓	✓
セキュリティコントロール						
デバイスコントロール	✓	✓	✓	✓	✓	✓
ウェブコントロール	✓	✓	✓	✓	✓	✓
データ暗号化						
FileVault ディスク暗号化	—	✓	✓	✓	✓	✓
Detection and Response						
Endpoint Detection and Response Optimum	—	—	—	✓	✓	—
Endpoint Detection and Response Expert	—	—	—	—	—	✓
Kaspersky Sandbox (Kaspersky Sandbox のライセンスは別途購入する必要があります)	✓	✓	✓	✓	✓	✓

標準タスクの実行

本製品の起動と終了

[すべて表示](#) | [すべて隠す](#)

Kaspersky Endpoint Security のインストールが完了すると、本製品が自動で起動し、メニューバーに[製品アイコン](#)が表示されます。

本製品を開く[?]

メニューバーにある本製品のアイコンをクリックし、**[Kaspersky Endpoint Security]** を選択します。

本製品の終了[?]

メニューバーにある本製品のアイコンをクリックし、**[終了]** を選択します。

本製品を終了すると、コンピュータのメモリから製品のプロセスが削除されます。

重要： Kaspersky Endpoint Security を終了するとコンピュータは保護されなくなるため、感染やデータの消失の危険性が発生する場合があります。

コンピュータの保護ステータスの表示

本製品の[メインウィンドウ](#)にある、盾の形状をしたコンピュータの保護ステータスインジケータは、コンピュータの保護の問題を示します。インジケータの色は、コンピュータの保護状態に応じて変わります。セキュリティ上の脅威が検知された場合、その脅威に関するメッセージがメインウィンドウに表示され、インジケータの色が変わります。

インジケータの色は次のように変化します：

- 緑：** コンピュータが適切に保護されています。
 緑のインジケータは、定義データベースが最新で、本製品のコンポーネントがカスペルスキーの推奨通りに設定されていることを表します。悪意のあるオブジェクトは検知されていないか、既に駆除されています。
- 黄：** 保護機能のレベルが低下しています。
 黄色のインジケータは、Kaspersky Endpoint Security が問題を検知していることを表します。検知される問題は、推奨される保護の設定とやや異なる状態、定義データベースがしばらくアップデートされていない状態などです。
- 赤：** コンピュータが感染する危険があります。
 赤いインジケータは、コンピュータの感染やデータ損失につながる可能性のある危険な問題があることを示します。たとえば、定義データベースが長期間アップデートされていない状態、本製品がアクティブされていない状態、悪意のあるオブジェクトが検知された状態などです。

可能な限り速やかに、問題を解決し、セキュリティ上の脅威に対応することを推奨します。

インストールされているコンポーネントの動作状況の表示

Kaspersky Endpoint Security では、インストールされているコンポーネントのステータスを **「セキュリティ」** ウィンドウで確認できます。各コンポーネントの名前に隣接するインジケータは、そのステータスを示します。

コンポーネントのステータスの表示

1. 本製品の [メインウィンドウ](#) を開きます。
2. 本製品のメインウィンドウのサイドバーで、**「セキュリティ」** をクリックします。
「セキュリティ」 ウィンドウが表示されます。

次のステータスインジケータが表示される場合があります：

-  コンポーネントが実行中です。
-  コンポーネントは実行されており、セキュリティポリシーによって管理されています。
-  コンポーネントに不具合が発生しました。
-  コンポーネントに不具合があり、セキュリティポリシーによって管理されています。
-  コンポーネントはオフになっています。
-  コンポーネントはオフになっており、セキュリティポリシーによって管理されています。
-  コンポーネントは一時停止されています。
-  このコンポーネントは、現在のライセンスではサポートされていません。

注意：コンポーネントによっては、コンポーネント名に隣接する三点メニューを使用してレポートを開いたり、コンポーネントを設定したりすることもできます。

保護機能の無効化および再開

既定では、オペレーティングシステムが起動すると Kaspersky Endpoint Security が起動し、コンピュータの電源が切れるまでコンピュータを保護します。すべての保護コンポーネント（ファイル脅威対策、ウェブ脅威対策、ネットワーク脅威対策）が有効化され、実行されます。

保護を完全に無効化することもできますし、特定の保護コンポーネントを無効にすることもできます。

重要：保護または保護コンポーネントは無効化しないことを強く推奨します。これらを無効にすると、コンピュータが感染し、データが失われる危険性があります。

コンピュータの保護が無効になっている場合：

- メニューバーにある [本製品のアイコン](#) が非アクティブ（グレー）になっている。
- メインウィンドウにある保護ステータスを示すインジケータが赤色になっている。

1つ以上の保護コンポーネントが無効になっている場合、保護ステータスを示すインジケータは赤色または黄色になります。

注意：保護機能を無効にしたり一時停止したりしても、[スキャン](#)や[アップデート](#)の実行には影響ありません。

コンピュータの保護を完全に無効または再開するには、次のいずれかの方法を使用してください。

- 製品アイコンから
- 本製品の設定ウィンドウから
- **「プロテクション」** のメニューから

[製品アイコンからコンピュータの保護機能は無効化または再開する](#)

1. メニューバーにある本製品のアイコンをクリックし、[保護機能を無効にする] または [保護機能を有効にする] を選択します。
保護を無効にすると、管理者の認証情報の入力が必要されます。
2. 管理者の認証情報の入力画面で管理者の名前とパスワードを入力し、Kaspersky Endpoint Security の保護の無効化を確認します。

本製品の設定ウィンドウからコンピュータの保護機能を無効化または再開する

1. メニューバーで製品アイコンをクリックし、[設定] を選択します。
本製品の設定ウィンドウが表示されます。
2. [脅威対策] タブの [全般] セクションで [保護機能を有効にする] をオンまたはオフにします。

メニューバーからコンピュータの保護機能を無効化または再開する

メニューバーで [プロテクション] → [保護機能を無効にする] / [保護機能を有効にする] をクリックします。

重要：コンピュータの保護を無効にした場合、Kaspersky Endpoint Security の再起動後に、コンピュータの保護が自動的に有効化されることはありません。手動でコンピュータの保護を再度有効にする必要があります。

保護コンポーネントを無効にする

1. メニューバーで製品アイコンをクリックし、[設定] を選択します。
本製品の設定ウィンドウが表示されます。
2. [脅威対策] タブの [<コンポーネント名>] セクションにある [<コンポーネント名> を有効にする] をオフにします。

重要：保護コンポーネントを無効にした場合、Kaspersky Endpoint Security の再起動後に、無効にしたコンポーネントが自動的に有効化されることはありません。手動で保護コンポーネントを再度有効にする必要があります。

保護コンポーネントを有効にするには：

1. メニューバーで製品アイコンをクリックし、[設定] を選択します。
本製品の設定ウィンドウが表示されます。
2. [脅威対策] タブの [<コンポーネント名>] セクションにある [<コンポーネント名> を有効にする] をオンにします。

プロテクションセンターでも、コンピュータの保護または保護機能を有効にすることができます。コンピュータの保護または保護コンポーネントを無効にすると、コンピュータの感染リスクが急速に高まります。そのため、コンピュータの保護が無効になると、プロテクションセンターで通知されます。

プロテクションセンターの使用

プロテクションセンターは、問題やコンピュータセキュリティへの脅威の分析と解決を支援する Kaspersky Endpoint Security の機能の1つです。

プロテクションセンターを開く

本製品の メインウィンドウ のサイドバーで、[プロテクションセンター] をクリックします。

プロテクションセンターで、アクティブな脅威についての情報を探し、定義データベースのステータスを確認し、保護コンポーネントが無効にされているかどうかを確認できます。

注意：組織のシステム管理者が危険な Web サイトへのアクセスのブロックをウェブコントロールで有効に設定している場合、プロテクションセンターに「**ウェブコントロールが有効です**」と通知が表示されます。

問題や脅威ごとに、推奨される対処方法が表示されます。たとえば、コンピュータで感染したファイルが検知された場合は、「**駆除**」をクリックします。定義データベースがアップデートされていない場合は、「**アップデート**」をクリックします。すぐに問題を解決したり、脅威を処理したりできます。これらの操作を後で実行することもできます。

問題や脅威をすぐに処理する

問題や脅威に対して推奨される対処方法のボタンをクリックします。

選択した処理が実行されます。

危険な脅威を処理せずにプロテクションセンターを閉じた場合、脅威が依然として残っていることを警告するために、メインウィンドウにある保護ステータスのインジケータは赤いままになります。

スキャンタスクの実行

既定の完全スキャンタスクは **Kaspersky Endpoint Security** に含まれています。このタスクを実行すると、コンピュータのメモリ、スタートアップオブジェクト、内蔵ディスクすべてがスキャンされ、ウイルスやマルウェアの有無がチェックされます。

コンピュータの完全スキャン

1. 本製品の メインウィンドウ のサイドバーで、「**スキャン**」をクリックします。
「**スキャン**」ウィンドウが表示されます。

2. 「**完全スキャン**」  をクリックします。

完全スキャンが開始されます。

既定の簡易スキャンタスクは **Kaspersky Endpoint Security** に含まれています。このタスクを実行すると、コンピュータの重要な部分（メモリ、スタートアップオブジェクト、システムフォルダ）がスキャンされ、ウイルスなどのマルウェアの有無がチェックされます。

コンピュータの簡易スキャン

1. 本製品の メインウィンドウ のサイドバーで、「**スキャン**」をクリックします。
「**スキャン**」ウィンドウが表示されます。

2. 「**簡易スキャン**」  をクリックします。

簡易スキャンが開始されます。

個々のオブジェクト（内部ドライブ、フォルダ、ファイル、リムーバブルディスクなど）にウイルスなどのマルウェアがないかスキャンする場合は、オブジェクトスキャンを実行します。

選択した項目のスキャン

次のいずれかを実行します：

- 選択したアイテムを右クリックし、「**マルウェアスキャン**」を選択します。
- 選択した項目をドラッグし、Dock の 製品アイコン にドロップします。
- 選択した項目をドラッグし、「**スキャン**」ウィンドウにドロップします。

完了したスキャンの結果は「**レポート**」ウィンドウで確認できます。

注意：Kaspersky Endpoint Security は、OneDrive や iCloud ストレージ、その他のクラウドストレージにあるファイルをスキャンしません。これらのファイルをスキャン範囲から除外してください。そうしないと、スキャンタスクが「感染したファイルが削除されませんでした」というエラーで終了する可能性があります。

スケジュール済みスキャンタスクの自動起動の設定

簡易スキャンタスクと完全スキャンタスクを開始するスケジュールを作成できます。設定したスケジュールに従って、コンピュータ全体またはコンピュータの重要な領域が自動的にスキャンされます。

[「スキャン」 ウィンドウからスキャンタスクをスケジュールする](#)

1. 本製品の[メインウィンドウ](#)のサイドバーで、**「スキャン」** をクリックします。
「スキャン」 ウィンドウが表示されます。
2. **「スキャンをスケジュールする」** をクリックします。
スケジュールを設定するダイアログが開きます。
3. **「完全スキャン」** または **「簡易スキャン」** をオンにします。
4. スキャンを開始する頻度と開始時刻を指定します。
5. **「OK」** をクリックします。

[「設定」 ウィンドウからスキャンタスクをスケジュールする](#)

1. メニューバーで製品アイコンをクリックし、**「設定」** を選択します。
本製品の設定ウィンドウが表示されます。
2. **「スキャン」** タブで、**「スケジュール」** をクリックします。
3. 表示されるウィンドウで、スケジュールを設定して開始させるスキャンの名前の隣のチェックボックスをオンにします。
4. スキャンタスクの頻度と日時を設定します。
5. **「OK」** をクリックして、スキャンタスクのスケジュールの変更内容を保存します。

スキャンタスクの結果は、**「レポート」** ウィンドウで確認できます。

定義データベースのアップデート

カスペルスキーのアップデートサーバが、Kaspersky Endpoint Security のアップデートの主な入手元です。アップデート元には、ディストリビューションポイント、ローカルフォルダおよびその他の Web サーバを使用することもできます。

注意：アップデートサーバからアップデートをダウンロードするにはインターネット接続が必要です。

既定では、カスペルスキーのアップデートサーバにあるアップデートを定期的に確認します。最新のアップデートがサーバにある場合は、バックグラウンドモードでダウンロードされ、コンピュータにインストールされます。

[Kaspersky Endpoint Security のアップデートを開始する](#)

1. 本製品の[メインウィンドウ](#)のサイドバーで、**「アップデート」** をクリックします。
「アップデート」 ウィンドウが表示されます。
2. **「アップデート」** をクリックします。
アップデートの有無が確認されます。アップデートがある場合、ダウンロードされ、コンピュータにインストールされます。

次のいずれかの方法でもアップデートタスクを開始できます。

- 製品アイコンをクリックし、**「アップデート」** を選択します。

- メニューバーで **「プロテクション」** → **「アップデート」** の順に選択します。

定義データベースをアップデートする方法を変更することができます。既定では、定義データベースは自動的にアップデートされます。

[定義データベースの自動アップデートを有効または無効にする](#)

1. メニューバーで製品アイコンをクリックし、**「設定」** を選択します。
本製品の設定ウィンドウが表示されます。
2. **「アップデート」** タブの **「定義データベース」** セクションで **「自動的にアップデートをダウンロードする」** をオンまたはオフにします。

完了したアップデートの結果は **「レポート」** ウィンドウで確認できます。

ご注意： アップデート機能（マルウェア対策の署名のアップデートおよびコードベースのアップデートの提供を含む）および KSN 機能は、アメリカ合衆国内にある本ソフトウェアではご利用いただけなくなる可能性があります。

ファイルアクセスがブロックされた場合の操作

[すべて表示](#) | [すべて隠す](#)

Kaspersky Endpoint Security は、感染したファイルやアプリケーションへのアクセスをブロックします。ファイルが感染した場合、アクセスする前に駆除する必要があります。

[検知したオブジェクトを駆除する](#)

1. メニューバーで **「プロテクション」** → **「検知したオブジェクト」** の順に選択します。
「検知したオブジェクト」 ウィンドウが開きます。
2. **「検知したオブジェクト」** セクションで、駆除が必要なファイルに隣接する *** をクリックし、**「駆除」** を選択します。
選択した脅威の駆除が開始されます。オブジェクトの駆除中に表示されるダイアログで、オブジェクトに対して実行する処理を選択できます。

[検知したオブジェクトをすべて駆除する](#)

1. メニューバーで **「プロテクション」** → **「検知したオブジェクト」** の順に選択します。
「検知したオブジェクト」 ウィンドウが開きます。
2. **「検知したオブジェクト」** セクションで、**「すべて駆除」** をクリックします。
検知した脅威の駆除が開始されます。オブジェクトの駆除中に表示される通知ウィンドウで、オブジェクトに対して実行する処理を選択できます。通知ウィンドウで処理を選択する時に **「選択した処理を常に実行」** をオンにすると、この種別のすべてのファイルに選択した処理が適用されます。

ファイル脅威対策によってブロックされたファイルが安全であることが確実な場合は、[信頼ゾーン](#)に登録できます。

削除または駆除されたファイルの復元

駆除処理中はファイル全体を保存できない場合があります。駆除後にファイルの一部または全部にアクセスできない場合は、バックアップから元のファイルの復元を試行できます。

[駆除中に削除または変更されたファイルを復元する](#)

1. メニューバーで **「プロテクション」** → **「検知したオブジェクト」** の順に選択します。
「検知したオブジェクト」 ウィンドウが開きます。
2. **「バックアップ」** セクションで、復元するファイルに隣接する *** をクリックします。
ポップアップメニューが表示されます。
3. **「ファイルを復元」** を選択します。

ファイル名、タグ、ファイルの復元先フォルダを指定するウィンドウが表示されます。既定では、元のファイル名と元の保存場所があらかじめ指定されています。

4. ファイル名とファイルの復元先のフォルダを指定します。

5. **〔保存〕** をクリックします。

ファイルは指定された場所に指定された名前で復元されます。

復元後には、すぐにファイルのマルウェアスキャンを実行してください。アップデートされた定義データベースでスキャンすることで、オブジェクトを破損させずに駆除できる可能性があります。

重要：コンピュータが感染する可能性があるため、どうしても必要である場合を除き、バックアップコピーからファイルを復元しないでください。

製品の動作レポートの表示

検知された全オブジェクトがリストされた Kaspersky Endpoint Security レポートが、**〔処理されたオブジェクト〕** タブに表示されます。システムイベントは、**〔システムイベント〕** タブに表示されます。また、次のコンポーネントごとの詳細レポートが作成されます：[ファイル脅威対策](#)、[ウェブ脅威対策](#)、[ネットワーク脅威対策](#)、[ふるまい検知](#)、[スキャンタスク](#)と[アップデートタスク](#)。

[「レポート」ウィンドウを表示する](#)

メニューバーで **〔プロテクション〕** → **〔レポート〕** の順に選択します。

通知ウィンドウが表示された場合の操作

ウィンドウ形式の通知は、ユーザに必ず読んでほしい製品イベントを知らせるものです。

通知ウィンドウが表示された場合は、提示されたオプションのいずれかを選択します。最適なオプションは、カスペルスキーのエキスパートにより既定として設定されたオプションです。

製品の詳細設定

コンピュータの保護対象

Kaspersky Endpoint Security が検知した脅威は、様々な属性に基づいて複数のカテゴリに分類されます。Kaspersky Endpoint Security では、ウイルス、ワーム、トロイの木馬、悪意のあるツールは常にスキャンします。マルウェアはコンピュータに多大な損害を与える可能性があります。保護機能の信頼性をさらに高めるために、コンピュータや個人情報に損害を与えるために悪用される可能性がある正規のプログラムのチェックを有効にして、検知するオブジェクトの範囲を広げることができます。

Kaspersky Endpoint Security が保護を提供するオブジェクトは、次のグループに分けられます：

- **ウイルス、ワーム、トロイの木馬、悪意のあるツール、アドウェア、オートダイヤラー：**

このカテゴリには次が該当します：

- すべての種別のマルウェア。
- コンピュータで広告（バナーなど）を表示したり、Web ブラウザでの検索結果を Web サイトの広告に置き換えたりして、ユーザに迷惑をかけるソフトウェア。
- 利用者の許可なくコンピュータのモデムによる電話回線接続を確立するアプリケーション。

あらゆるマルウェアから保護することで、必要最低限の安全性を確保できます。カスペルスキーが推奨する設定に基づき、このカテゴリに属するオブジェクトは常に監視されます。

- **ユーザに損害を与える目的で悪用される可能性がある正規のソフトウェア：**このカテゴリには、侵入者がユーザのコンピュータやデータに損害を与えるために悪用する可能性のある正規のアプリケーション（リモート管理アプリケーションなど）が含まれます。

[検知するオブジェクトのカテゴリの選択](#)

1. メニューバーで製品アイコンをクリックし、**〔設定〕** を選択します。

本製品の設定ウィンドウが表示されます。

2. **〔脅威〕** タブの **〔検知するオブジェクト〕** セクションで、検知するオブジェクトが属するカテゴリに隣接するチェックボックスをオンにします。

注意：ユーザのコンピュータは、ウイルス、ワーム、トロイの木馬、悪意のあるツール、オートダイアラーからは常に保護されます。したがって、このカテゴリのチェックボックスをオフにすることはできません。

ファイル脅威対策、ウェブ脅威対策、スキャンタスクの実行中は、選択した検知対象のオブジェクトのカテゴリに基づいて、一部またはすべての定義データベースが使用されます。

注意：Kaspersky Endpoint Security によってマルウェアに分類されたアプリケーションが安全であるという確証がある場合、そのアプリケーションを信頼ゾーンに追加できます。

信頼ゾーンは、スキャンや監視の対象外となるオブジェクトのリストです。たとえば、無害であることが確実なオブジェクトやアプリケーション、URL へのアクセスがブロックされる場合は、これらを信頼ゾーンに追加することができます。

アプリケーションを信頼ゾーンに追加した場合、アプリケーションのファイルやネットワークにおける動作は、疑わしい動作も含め、一切監視されなくなります。ただし、信頼するアプリケーションであっても、実行ファイルとプロセスのスキャンは続行されます。

注意：管理者が信頼ゾーンの編集を禁止するようにポリシーを設定すると、ユーザは信頼ゾーンの設定に移動できなくなります。

信頼するファイルとフォルダのリストにファイルやフォルダを追加または削除する

1. メニューバーで製品アイコンをクリックし、**〔設定〕** を選択します。
本製品の設定ウィンドウが表示されます。
2. **〔脅威〕** タブの **〔除外〕** セクションにある **〔信頼ゾーン〕** をクリックします。
信頼ゾーンの設定ウィンドウが表示されます。
3. **〔ファイルとフォルダ〕** タブで、信頼するファイルとフォルダのリストを編集します：
 - ファイルまたはフォルダをリストに追加するには：
 - a. **+** をクリックします。
ダイアログが表示されます。ここから、ファイルまたはフォルダを選択することができます。
 - b. 追加するファイルまたはフォルダを選択します。
 - c. **〔開く〕** をクリックします。
 - ファイルまたはフォルダをリストから削除するには：
 - a. 信頼するファイルとフォルダのリストから削除するファイルまたはフォルダを選択します。
 - b. **–** をクリックします。
4. **〔OK〕** をクリックします。

信頼する URL のリストで信頼する URL を追加または削除する

1. メニューバーで製品アイコンをクリックし、**〔設定〕** を選択します。
本製品の設定ウィンドウが表示されます。
2. **〔脅威〕** タブの **〔除外〕** セクションにある **〔信頼ゾーン〕** をクリックします。
信頼ゾーンの設定ウィンドウが表示されます。
このウィンドウは、**〔信頼ゾーン〕** タブの **〔全般〕** セクションにある **〔脅威対策〕** をクリックして開くこともできます。
3. **〔URL〕** タブで、信頼済みの Web サイトのアドレスのリストを編集します：
 - リストに URL を追加するには：
 - a. **+** をクリックします。
 - b. リストに追加する URL を入力します。

c. **[OK]** をクリックします。

- リストからアドレスを削除するには：

a. 削除したい URL を選択します。

b. **–** をクリックします。

4. **[OK]** をクリックします。

既定では、信頼する URL のリストは空です。

信頼済みアプリケーションのリストで信頼済みアプリケーションを追加または削除する ②

1. メニューバーで製品アイコンをクリックし、**[設定]** を選択します。

本製品の設定ウィンドウが表示されます。

2. **[脅威]** タブの **[除外]** セクションにある **[信頼ゾーン]** をクリックします。

信頼ゾーンの設定ウィンドウが表示されます。

このウィンドウは、**[信頼ゾーン]** タブの **[全般]** セクションにある **[脅威対策]** をクリックして開くこともできます。

3. **[信頼済みアプリケーション]** タブで、信頼済みアプリケーションのリストを編集します。

- リストにアプリケーションを追加するには：

a. **+** をクリックします。

必要なアプリケーションのパラメータを指定できるウィンドウが開きます。

b. 追加するアプリケーションの次のパラメータを指定します：

- **パス**
- **コード署名の要件**

注意：これら 2 つのパラメータの値を手動で入力するか、**[選択]** をクリックして、開いたウィンドウで追加するアプリケーションを選択できます。この場合、これらのパラメータの値が自動的に挿入されます。

c. **[オプション]** セクションで、Kaspersky Endpoint Security アプリケーションで監視しない活動の種別を少なくとも 1 つ選択します：

- **ファイル操作を監視しない**
- **ネットワーク活動を監視しない**

d. **[OK]** をクリックします。

- リストからアプリケーションを削除するには：

a. 削除するオブジェクトを選択します。

b. **–** をクリックします。

既定では、信頼するアプリケーションのリストは空です。

信頼済みアプリケーションを編集する ②

1. メニューバーで製品アイコンをクリックし、**[設定]** を選択します。

本製品の設定ウィンドウが表示されます。

2. **[脅威]** タブの **[除外]** セクションにある **[信頼ゾーン]** をクリックします。

信頼ゾーンの設定ウィンドウが表示されます。

このウィンドウは、**[信頼ゾーン]** タブの **[全般]** セクションにある **[脅威対策]** をクリックして開くこともできます。

3. **[信頼済みアプリケーション]** タブで、編集するアプリケーションを選択します。

4. **[編集]** をクリックします。
5. 表示されるウィンドウで、アプリケーションのパラメータを編集します。
6. **[OK]** をクリックします。

信頼する URL の監視を有効にする

1. メニューバーで製品アイコンをクリックし、**[設定]** を選択します。
本製品の設定ウィンドウが表示されます。
2. **[脅威]** タブの **[除外]** セクションにある **[信頼ゾーン]** をクリックします。
信頼ゾーンの設定ウィンドウが表示されます。
3. **[URL]** タブで、Kaspersky Endpoint Security が監視する URL に隣接するチェックボックスをオフにします。
4. **[OK]** をクリックします。

ファイル脅威対策

ファイル脅威対策は、コンピュータのファイルシステムを感染から保護します。このコンポーネントは、オペレーティングシステムの起動中に開始され、コンピュータのメモリに常駐します。そして、コンピュータ上およびすべての接続されているディスク上で開かれるファイル、保存されるファイル、実行されるファイルのすべてをスキャンし、マルウェアを検知します。ファイル脅威対策を無効にすると、オペレーティングシステムの起動時に開始されません。手動でファイル脅威対策を再度有効にする必要があります。

ファイル脅威対策を有効または無効にする

1. メニューバーで製品アイコンをクリックし、**[設定]** を選択します。
本製品の設定ウィンドウが表示されます。
2. **[脅威対策]** タブの **[ファイル脅威対策]** セクションで、**[ファイル脅威対策を有効にする]** をオンまたはオフにします。
[プロテクションセンター](#)でもファイル脅威対策を有効にできます。コンピュータの保護または保護コンポーネントを無効にすると、コンピュータの感染リスクが急速に高まります。そのため、保護が無効になると、プロテクションセンターで通知されます。

ファイル脅威対策の範囲を作成できます。

ファイルやフォルダを保護範囲に追加または保護範囲から削除する

1. メニューバーで製品アイコンをクリックし、**[設定]** を選択します。
本製品の設定ウィンドウが表示されます。
2. **[脅威対策]** タブで、**[ファイル脅威対策]** セクションの **[保護範囲]** をクリックします。
ファイル脅威対策のスキャン対象のオブジェクトのリストが、ウィンドウに表示されます。既定では、ファイル脅威対策は、コンピュータに接続されている内部ディスク、リムーバブルディスク、およびネットワークドライブにあるすべてのオブジェクトをスキャンします。

ご注意：読み取り専用のシステムボリュームのスキャンをスキップして、スキャン時間を大幅に短縮することができます。既定では、ファイル脅威対策は、読み取り専用のシステムボリュームをスキャンしません。

3. **[保護範囲]** セクションで、保護範囲へのオブジェクトの追加、保護範囲からのオブジェクトの削除を行います。
 - 保護範囲にファイルまたはフォルダを追加するには：
 - a. **+** をクリックします。
ドロップダウンリストが表示されます。ここから、保護範囲に追加するオブジェクトを選択できます。
 - b. ドロップダウンリストで、**[ファイルとフォルダ]** を選択します。
ダイアログが表示されます。ここから、ファイルまたはフォルダを選択することができます。
 - c. 保護範囲に追加するファイルまたはフォルダを選択します。

d. **〔開く〕** をクリックします。

- 保護範囲からファイルやフォルダを削除するには：

a. 保護範囲に含まれるオブジェクトのリストから目的のオブジェクトを選択します。

b. 選択したオブジェクトをウインドウからドラッグするか、**－** をクリックします。

4. 読み取り専用のシステムボリュームをスキャンする場合は、**〔最適化〕** セクションで **〔読み取り専用のシステムボリュームのスキャンをスキップする〕** をオフにします。

重要：最適化の操作が、セキュリティ上の理由から無効化される場合があります。

5. **〔保存〕** をクリックします。

既定のオブジェクトリストのオブジェクトを保護範囲に追加または保護範囲から削除する

1. メニューバーで製品アイコンをクリックし、**〔設定〕** を選択します。

本製品の設定ウインドウが表示されます。

2. **〔脅威対策〕** タブで、**〔ファイル脅威対策〕** セクションの **〔保護範囲〕** をクリックします。

ファイル脅威対策のスキャン対象のオブジェクトのリストが、ウインドウに表示されます。既定では、ファイル脅威対策は、コンピュータに接続されている内部ディスク、リムーバブルディスク、およびネットワークドライブにあるすべてのオブジェクトをスキャンします。

ご注意：読み取り専用のシステムボリュームのスキャンをスキップして、スキャン時間を大幅に短縮することができます。既定では、ファイル脅威対策は、読み取り専用のシステムボリュームをスキャンしません。

3. 既定のオブジェクトリストのオブジェクトを**保護範囲**に追加または保護範囲から削除する：

- 既定のオブジェクトリストのオブジェクトを保護範囲に追加するには：

a. **+** をクリックします。

ドロップダウンリストが表示されます。ここから、保護範囲に追加するオブジェクトを選択できます。

b. ドロップダウンリストで、保護範囲に追加するオブジェクト (**〔すべての内部ディスク〕** など) を選択します。

- 既定のオブジェクトリストのオブジェクトを保護範囲から削除するには：

a. 保護範囲に含まれるオブジェクトのリストから目的のオブジェクトを選択します。

b. 選択したオブジェクトをウインドウからドラッグするか、**－** をクリックします。

4. 読み取り専用のシステムボリュームをスキャンする場合は、**〔最適化〕** セクションで **〔読み取り専用のシステムボリュームのスキャンをスキップする〕** をオフにします。

重要：最適化の操作が、セキュリティ上の理由から無効化される場合があります。

5. **〔保存〕** をクリックします。

保護範囲内でオブジェクトの保護を無効にする

1. メニューバーで製品アイコンをクリックし、**〔設定〕** を選択します。

本製品の設定ウインドウが表示されます。

2. **〔脅威対策〕** タブで、**〔ファイル脅威対策〕** セクションの **〔保護範囲〕** をクリックします。

ファイル脅威対策のスキャン対象のオブジェクトのリストが、ウインドウに表示されます。既定では、ファイル脅威対策は、コンピュータに接続されている内部ディスク、リムーバブルディスク、およびネットワークドライブにあるすべてのオブジェクトをスキャンします。

ご注意：読み取り専用のシステムボリュームのスキャンをスキップして、スキャン時間を大幅に短縮することができます。既定では、ファイル脅威対策は、読み取り専用のシステムボリュームをスキャンしません。

3. 保護範囲に含まれるオブジェクトのリストで、目的のオブジェクトに隣接するチェックボックスをオフにします。
4. **〔保存〕** をクリックします。

読み取り専用のシステムボリュームのスキャンを有効にする

1. メニューバーで製品アイコンをクリックし、**〔設定〕** を選択します。
本製品の設定ウィンドウが表示されます。

2. **〔脅威対策〕** タブで、**〔ファイル脅威対策〕** セクションの **〔保護範囲〕** をクリックします。
ファイル脅威対策のスキャン対象のオブジェクトのリストが、ウィンドウに表示されます。既定では、ファイル脅威対策は、コンピュータに接続されている内部ディスク、リムーバブルディスク、およびネットワークドライブにあるすべてのオブジェクトをスキャンします。

ご注意：読み取り専用のシステムボリュームのスキャンをスキップして、スキャン時間を大幅に短縮することができます。既定では、ファイル脅威対策は、読み取り専用のシステムボリュームをスキャンしません。

3. **〔最適化〕** セクションで、**〔読み取り専用のシステムボリュームのスキャンをスキップする〕** をオフにします。

重要：最適化の操作が、セキュリティ上の理由から無効化される場合があります。

4. **〔保存〕** をクリックします。

ユーザまたはアプリケーションが、保護範囲に含まれるファイルにアクセスしようとする、ファイル脅威対策が iSwift のデータベースでこのファイルについての情報を確認し、その情報を使用して、ファイルをスキャンする必要があるかどうかを判断します。

悪意のあるオブジェクトは、シグネチャ分析によって検知されます。この方法では、定義データベースに含まれる脅威の説明に基づいて、脅威が検索されます。シグネチャ分析に加え、ファイル脅威対策はヒューリスティック分析やその他のスキャン技術を使用します。

ファイルで脅威を検知した場合は、検知したマルウェアの種別（たとえば「ウイルス」や「トロイの木馬」）が特定されます。その後、検知したオブジェクトに関する通知が表示され、ファイル脅威対策の設定に基づいて、そのオブジェクトが処理されます。

感染したファイルの検知時にファイル脅威対策が実行する処理を選択する

1. メニューバーで製品アイコンをクリックし、**〔設定〕** を選択します。
本製品の設定ウィンドウが表示されます。
2. **〔脅威対策〕** タブの **〔ファイル脅威対策〕** セクションで、感染したファイルの検知後にファイル脅威対策が実行する処理を選択します。

感染したファイルを駆除または削除する前に、Kaspersky Endpoint Security はバックアップコピーを保存し、後で復元または駆除できるようにします。

ファイル脅威対策と検知したすべての脅威の情報はレポートに記録されます。

注意：ファイル脅威対策がエラーを表示して停止した場合は、レポートを確認してコンポーネントを再起動してください。問題が解決されない場合は、[カスペルスキーのテクニカルサポートにお問い合わせください](#)。

ファイル脅威対策のレポートの表示

1. メニューバーで **〔プロテクション〕** → **〔レポート〕** の順に選択します。
〔レポート〕 ウィンドウが表示されます。
2. **〔ファイル脅威対策〕** タブを開きます。

ウェブ脅威対策

インターネットの使用時、コンピュータはマルウェアによる感染リスクやその他のセキュリティ上の脅威にさらされています。コンピュータのセキュリティ上の脅威は、無料プログラムをダウンロードしたり、ハッカーに攻撃された Web サイトへアクセスしたりした時に、コンピュータへ侵入する可能性があります。また、コンピュータがインターネット接続を確立した直後、Web アドレスを開いたりファイルをダウンロードしたりする前に、ネットワークワームがコンピュータを攻撃する可能性があります。

Kaspersky Endpoint Security は、コンピュータが HTTP および HTTPS プロトコルを使用して Safari、Chrome、Firefox 経由で送受信する情報を保護します。

注意：Kaspersky Endpoint Security は、HTTP および HTTPS プロトコルを使用したデータ転送に使われる頻度が最も高いポートで Web トラフィックを監視します。[全般] セクションの [セキュアな接続 (HTTPS) をチェックする] をオンにしている場合にのみ、暗号化された接続がスキャンされます。

ウェブ脅威対策を有効または無効にする ②

1. メニューバーで製品アイコンをクリックし、[設定] を選択します。
本製品の設定ウィンドウが表示されます。
2. [脅威対策] タブの [ウェブ脅威対策] セクションで、[ウェブ脅威対策を有効にする] をオンまたはオフにします。

[プロテクションセンター](#)でもウェブ脅威対策を有効にできます。コンピュータの保護または保護コンポーネントを無効にすると、コンピュータの感染リスクが急速に高まります。そのため、保護が無効になると、プロテクションセンターで通知されます。

重要：ウェブ脅威対策を無効にした場合、Kaspersky Endpoint Security の再起動後に、ウェブ脅威対策が自動的に有効になることはありません。手動でウェブ脅威対策を再度有効にする必要があります。

ウェブ脅威対策は、カスペルスキーの推奨設定に基づいて、Web トラフィックをスキャンします。シグネチャ分析、ヒューリスティック分析、および [Kaspersky Security Network](#) からのデータを使用して悪意のあるオブジェクトが識別されます。

Web サイトのリンク先がフィッシングサイトや悪意のあるアドレスでないかどうかを確認することでフィッシング攻撃を回避できます。フィッシング攻撃では、通常、金融機関（銀行など）を装った犯罪者から、偽の Web サイトへのリンクが記載されたメールが送られてきます。このようなメールで、犯罪者はユーザを巧みに誘導して、フィッシングサイトにアクセスさせ、機密情報（キャッシュカードの番号や、オンラインバンキング口座の名義、パスワードなど）を入力させようとします。フィッシング攻撃では、たとえば、公式 Web サイトへのリンクを含む銀行からのお知らせに見せかけたメールが届きます。そのリンクは、実際には、詐欺の目的で作成された銀行の公式 Web サイトのコピーに向けられています。

ウェブ脅威対策はフィッシングサイトへアクセスしようとしていないかどうか、ユーザの Web トラフィックを監視し、このような Web サイトへのアクセスをブロックします。Web サイトのリンク先がフィッシングサイトや悪意のあるアドレスでないかどうかを確認するために、Kaspersky Endpoint Security は、定義データベース、ヒューリスティック分析および [Kaspersky Security Network](#) からのデータを使用します。

Web トラフィックのスキャンアルゴリズム

ユーザまたはアプリケーションが HTTP プロトコルや HTTPS プロトコルを使用してアクセスした Web サイトまたはファイルは、ウェブ脅威対策によって監視され、悪意のあるコードが含まれていないかスキャンされます。

- Web サイトやファイルに悪意のあるコードが含まれている場合、Kaspersky Endpoint Security が該当の Web サイトまたはファイルをブロックし、要求されたファイルまたは Web サイトが感染していることを知らせる通知が表示されます。
- ファイルまたは Web サイトに悪意のあるコードが含まれない場合は、すぐにアクセスできます。

危険な Web トラフィックオブジェクトが検知された時に、ウェブ脅威対策に実行させる処理を選択する ②

1. メニューバーで製品アイコンをクリックし、[設定] を選択します。
本製品の設定ウィンドウが表示されます。
2. [脅威対策] タブの [ウェブ脅威対策] セクションで、危険な Web トラフィックオブジェクトの検知後にウェブ脅威対策が実行する処理を選択します。

ウェブ脅威対策の動作に関する情報、および検知されたすべての危険な Web トラフィックオブジェクトはレポートに記録されます。

注意：ウェブ脅威対策がエラーを表示して停止した場合は、ウェブ脅威対策のレポートを確認してコンポーネントを再起動してください。問題が解決されない場合は、[カスペルスキーのテクニカルサポート](#)にお問い合わせください。

ウェブ脅威対策のレポートの表示 ②

1. メニューバーで **［プロテクション］** → **［レポート］** の順に選択します。
［レポート］ ウィンドウが表示されます。
2. **［ウェブ脅威対策］** タブを開きます。

メール脅威対策

メール脅威対策コンポーネントは、送受信メールの添付ファイルをスキャンして、マルウェアやその他の脅威を検出します。このコンポーネントは、定義データベース、Kaspersky Security Network クラウドサービス、ヒューリスティック分析を利用してコンピューターを保護します。

アプリケーションは、メールクライアント Apple Mail、Microsoft Outlook、Mozilla Thunderbird、Canary Mail、Spark、Mimestream、Airmail、Post Box、Boxy Suite 2、Twobird、Shift、Clean Email、eM Client、Superhuman、Polymail、HEY、Mail+ for Gmail、Spike mail をサポートしています。

既定では、メール脅威対策が有効になっています。必要に応じてメール脅威対策を無効にすることができます。

Web コンソールを使用してメール脅威対策を有効/無効にする ②

1. Web コンソールのメインウィンドウで、**［アセット（デバイス）］** → **［ポリシーとプロファイル］** の順に選択します。
2. Kaspersky Endpoint Security ポリシーの名前をクリックします。
ポリシーのプロパティウィンドウが表示されます。
3. **［アプリケーション設定］** タブを選択します。
4. **［脅威対策］** - **［メール脅威対策］** の順に選択します。
5. **［メール脅威対策］** スイッチをオンまたはオフにします。
6. メール脅威対策が有効になっている場合は、マルウェアが検出された場合にアプリケーションによって実行される処理を選択します。
 - 削除
 - ブロック
7. 必要に応じて、**詳細設定** セクションで、アーカイブのチェックの制限時間またはスキャンするアーカイブの最大サイズを設定します。
8. 変更を保存します。

管理コンソールを使用してメール脅威保護を有効/無効にする ②

1. 管理コンソールを起動します。
2. **［管理サーバー - <サーバ名>］** フォルダを展開します。
3. コンソールツリーで、**［管理対象デバイス］** をクリックします。
4. 作業領域で、**［ポリシー］** タブを選択します。
5. 設定するポリシーを右クリックして **［プロパティ］** を選択します。
6. **［プロパティ］** ウィンドウで、**［脅威対策］** - **［メール脅威対策］** の順に選択します。
7. **［メール脅威対策を有効にする］** をオンまたはオフにします。
8. **［脅威の検知時の処理］** セクションで、Kaspersky Endpoint Security が脅威を検出したときに実行する処理を選択します。
9. 必要に応じて、**メール脅威対策の設定** セクションで、アーカイブのチェックの制限時間またはスキャンするアーカイブの最大サイズを設定します。

10. [OK] をクリックして変更を保存します。

11. 次のいずれかを選択し、ポリシーに変更を適用します：

- [適用] をクリックし、**ポリシーのプロパティ** ウィンドウが開いたままの状態に変更を保存します。
- [OK] をクリックし、変更を保存して**ポリシーのプロパティ** ウィンドウを閉じます。

Kaspersky Endpoint Security を使用してメール脅威対策を有効または無効にする

1. メニューバーで製品アイコンをクリックし、[設定] を選択します。
本製品の設定ウィンドウが表示されます。
2. [脅威対策] タブの [メール脅威対策] セクションで、[メール脅威対策を有効にする] をオンまたはオフにします。
3. [メール脅威対策を有効にする] がオンになっている場合は、Kaspersky Endpoint Security が脅威を検出したときに実行する処理を選択します。
4. 必要に応じて、アーカイブのチェックの制限時間やスキャンするアーカイブの最大サイズを設定します。

メール脅威対策のレポートの表示

1. メニューバーで [プロテクション] → [レポート] の順に選択します。
[レポート] ウィンドウが表示されます。
2. [メール脅威対策] タブを開きます。

ネットワーク脅威対策

Kaspersky Endpoint Security は、コンピュータをネットワーク攻撃から保護します。

ネットワーク攻撃とは、リモートコンピュータのオペレーティングシステムに侵入する試みです。ネットワーク攻撃により、オペレーティングシステムが操作されたり、オペレーティングシステムのサービス妨害が発生したり、機密情報にアクセスされたりします。攻撃者は、これらの目的を達成するため、ポートスキャンや総当たり攻撃といった直接的な攻撃を実行したり、攻撃を受けているコンピュータにインストールされたマルウェアを使用したりします。

ネットワーク攻撃は、次の種別に分類されます：

- **ポートスキャン**：この種別のネットワーク攻撃は、通常は、より危険性が高いネットワーク攻撃の準備として実行されます。侵入者は、標的としたコンピュータでネットワークサービスを使用する UDP / TCP ポートをスキャンし、今後実行しようとしているより危険度が高い種別のネットワーク攻撃に対する脆弱性を判断します。また、ポートスキャンにより、侵入者は標的となるコンピュータのオペレーティングシステムの種別を判別し、その種別のオペレーティングシステムに適したネットワーク攻撃を選択できます。

- **DoS 攻撃**（サービス拒否状態を発生させるネットワーク攻撃）：このネットワーク攻撃では、標的となるオペレーティングシステムが不安定な状態になったり、完全に動作しなくなったりします。

DoS 攻撃の主な種別は次の通りです：

- 標的のコンピュータが予期していない特別に設計されたネットワークパケットを送りつけ、オペレーティングシステムの誤動作またはクラッシュを引き起こす攻撃。
- 短時間に大量のネットワークパケットをリモートコンピュータに送信する攻撃。標的となったコンピュータのすべてのリソースが、侵入者から送信されたネットワークパケットの処理に使用されます。その結果、コンピュータの機能が停止します。
- **ネットワーク侵入攻撃**：このネットワーク攻撃は、標的となるコンピュータのオペレーティングシステムを「乗っ取る」ことを目的としています。攻撃に成功すると、侵入者はオペレーティングシステムを完全に操作できるようになるため、これは最も危険な種別のネットワーク攻撃です。

この種別のネットワーク攻撃は、侵入者がリモートコンピュータから機密データ（クレジットカードの番号やパスワードなど）を取得する場合や、何らかの目的（そのコンピュータから、さらに別のコンピュータを攻撃するなど）でそのリモートコンピュータを密かに使用する場合に行われます。

ネットワーク脅威対策を有効または無効にする

1. メニューバーで製品アイコンをクリックし、[設定] を選択します。
本製品の設定ウィンドウが表示されます。

2. **[脅威対策]** タブの **[ネットワーク脅威対策]** セクションで、**[ネットワーク脅威対策を有効にする]** をオンまたはオフにします。

プロテクションセンターでもネットワーク脅威対策を有効にできます。コンピュータの保護または保護コンポーネントを無効にすると、コンピュータの感染リスクが急速に高まります。そのため、保護が無効になると、プロテクションセンターで通知されます。

重要：ネットワーク脅威対策を無効にした場合、Kaspersky Endpoint Security の再起動後に、ネットワーク脅威対策が自動的に有効になることはありません。手動でネットワーク脅威対策を再度有効にする必要があります。

危険なネットワーク活動を検知した Kaspersky Endpoint Security は、攻撃しているコンピュータが信頼するコンピュータのリストに登録されていない限り、そのコンピュータの IP アドレスを自動的にブロック対象のコンピュータリストに追加します。

ブロック対象のコンピュータのリストを編集する

1. メニューバーで製品アイコンをクリックし、**[設定]** を選択します。
本製品の設定ウィンドウが表示されます。
2. **[脅威対策]** タブの **[ネットワーク脅威対策]** セクションで、**[ネットワーク脅威対策を有効にする]** をオンにします。
3. **[設定]** をクリックします。
信頼するコンピュータのリストとブロック対象のコンピュータのリストが含まれたウィンドウが表示されます。
4. **[ブロック対象コンピュータ]** タブを開きます。
5. ブロックしたコンピュータが脅威ではないと確信している場合は、リストからそのコンピュータの IP アドレスを選択し、**[ブロック解除]** をクリックします。
確認ダイアログが開きます。
6. 確認ダイアログで、次のいずれかを選択します：
 - コンピュータのブロックを解除する場合は、**[ブロック解除]** をクリックします。
IP アドレスがブロック解除されます。
 - 選択した IP アドレスを常に許可する場合は、**[ブロック解除および信頼]** をクリックします。
IP アドレスがブロック解除され、信頼するコンピュータのリストに追加されます。
7. **[保存]** をクリックします。

信頼するコンピュータのリストを作成、編集することができます。Kaspersky Endpoint Security は、このリストに含まれるコンピュータからの危険なネットワーク活動を検知した場合でも、それらの IP アドレスを自動的にブロックしません。

信頼するコンピュータのリストを編集する

1. メニューバーで製品アイコンをクリックし、**[設定]** を選択します。
本製品の設定ウィンドウが表示されます。
2. **[脅威対策]** タブの **[ネットワーク脅威対策]** セクションで、**[ネットワーク脅威対策を有効にする]** をオンにします。
3. **[設定]** をクリックします。
信頼するコンピュータのリストとブロック対象のコンピュータのリストが含まれたウィンドウが表示されます。
4. **[信頼済みコンピュータ]** タブを開きます。
5. 信頼するコンピュータの IP アドレスを編集する：
 - 信頼するコンピュータのリストに IP アドレスを追加するには：
 - a. **+** をクリックします。
 - b. 表示される欄をクリックし、安全であると信頼できるコンピュータの IP アドレスを入力します。
 - 信頼するコンピュータのリストから IP アドレスを削除するには：
 - a. リストから IP アドレスを選択します。

b. – をクリックします。

- 信頼するコンピュータのリストにある IP アドレスを編集するには：

a. リストから IP アドレスを選択します。

b. **[編集]** をクリックします。

c. IP アドレスを変更します。

6. **[保存]** をクリックします。

Kaspersky Endpoint Security は、ネットワーク攻撃を検知すると、その攻撃に関する情報をレポートに記録します。

注意：ネットワーク脅威対策がエラーで実行を停止した場合は、レポートを確認してから、このコンポーネントを再起動してください。問題が解決されない場合は、[カスペルスキーのテクニカルサポート](#)にお問い合わせください。

ネットワーク脅威対策のレポートの表示^②

1. メニューバーで **[プロテクション]** → **[レポート]** の順に選択します。
[レポート] ウィンドウが表示されます。
2. **[ネットワーク脅威対策]** タブを開きます。

ファイアウォール

インターネットまたはローカルネットワークでの作業時に、ファイアウォールによって、コンピュータへの不正な接続がブロックされます。ファイアウォールは、コンピュータ上のアプリケーションのネットワーク動作も制御します。これにより、個人情報の盗難やその他の攻撃から企業 LAN を保護できます。このコンポーネントは、定義データベース、Kaspersky Security Network クラウドサービス、および事前定義されたネットワークルールを使用してコンピュータを保護します。

ネットワークルールの優先度

それぞれのルールには優先度が割り当てられています。ルールのリスト上の位置が高くなるほど、優先度が高くなります。ネットワーク動作が複数のルールに追加された場合、ファイアウォールは、最も優先度の高いルールに従ってネットワーク動作を制限します。

ネットワーク接続の種別

ファイアウォールを使用すると、ネットワーク接続の種別に応じてネットワーク動作を制御できます。Kaspersky Endpoint Security の設定でネットワーク接続の種別を変更できます。

使用可能なネットワーク接続の種別は次の通りです：

- **パブリックネットワーク：**ネットワークは、マルウェア対策アプリケーション、ファイアウォール、またはフィルターによって保護されていません（カフェの Wi-Fi など）。ユーザがこのようなネットワークに接続されているコンピュータを操作すると、ファイアウォールはこのコンピュータのファイルやプリンターへのアクセスをブロックします。外部ユーザは、共有フォルダからデータにアクセスすることも、このコンピュータのデスクトップにリモートアクセスすることもできません。ファイアウォールは、既定でインターネットにパブリックネットワークの種別を割り当てます。インターネットの種別を変更することはできません。
- **プライベートネットワーク：**このコンピュータ上のファイルやプリンターへのアクセスが制限されているユーザのネットワーク（企業 LAN やホームネットワークなど）。
- **信頼するネットワーク：**コンピュータが攻撃や不正なデータアクセスの危険にさらされていない安全なネットワーク。このステータスのネットワーク内では、ファイアウォールは、すべてのネットワーク動作を許可します。

管理コンソールでのファイアウォールの管理^②

1. 管理コンソールを起動します。
2. **[管理サーバ - <サーバ名>]** フォルダを展開します。
3. コンソールツリーで、**[管理対象デバイス]** をクリックします。
4. 作業領域で、**[ポリシー]** タブを選択します。

5. 設定するポリシーを右クリックして **プロパティ** を選択します。
6. **プロパティ** ウィンドウで、**脅威対策** → **ファイアウォール** の順に選択します。
7. **ファイアウォールを有効にする** をオンまたはオフにします。
8. **ファイアウォールの設定** セクションで、**設定** をクリックし、ルールを追加、編集、削除したり、ルールの優先度を変更したりします。
9. **使用可能なネットワーク** セクションで、**設定** をクリックし、ネットワークの種別を追加、編集、削除、または変更します。
10. **OK** をクリックして変更を保存します。
11. 次のいずれかを選択し、ポリシーに変更を適用します：
 - **適用** をクリックし、**ポリシーのプロパティ** ウィンドウが開いたままの状態に変更を保存します。
 - **OK** をクリックし、変更を保存して**ポリシーのプロパティ** ウィンドウを閉じます。

Web コンソールでのファイアウォールの管理

1. Web コンソールのメインウィンドウで、**アセット (デバイス)** → **ポリシーとプロファイル** の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
ポリシーのプロパティ ウィンドウが表示されます。
3. **アプリケーション設定** タブを選択します。
4. **脅威対策** → **ファイアウォール** の順に移動します。
5. **ファイアウォール** スイッチをオンまたはオフにします。
6. **ファイアウォールの設定** セクションで、**ネットワークパケットルール** をクリックし、ルールを追加、編集、削除したり、ルールの優先度を変更したりします。
7. **使用可能なネットワーク** セクションで、**ネットワーク設定** をクリックし、ネットワークの種別を追加、編集、または変更します。
8. 変更を保存します。

Kaspersky Endpoint Security でのファイアウォールの管理

1. メニューバーで製品アイコンをクリックし、**設定** を選択します。
本製品の設定ウィンドウが表示されます。
2. **脅威対策** タブの **ファイアウォール** セクションで **ファイアウォールを有効にする** をオンまたはオフにします。
3. 必要に応じて、**設定** をクリックし、ファイアウォールを設定します：
 - **ネットワークパケットルール** タブでは、ルールの追加、編集、削除、またはルールの優先度の変更ができます。
 - **使用可能なネットワーク** タブでは、ネットワークの種別を追加、編集、または変更できます。

これにより、ファイアウォールが有効になると、Kaspersky Endpoint Security がネットワーク動作を制御して、コンピュータへの不正なネットワーク接続をブロックします。

ファイアウォールのレポートの表示

1. メニューバーで **プロテクション** → **レポート** の順に選択します。
レポート ウィンドウが表示されます。
2. **ファイアウォール** タブを開きます。

ふるまい検知コンポーネントは、コンピュータ上のアプリケーションの動作に関するデータを受信し、この情報を他の保護コンポーネントに提供して、パフォーマンスを向上させます。ふるまい検知コンポーネントは、アプリケーションの Behavior Stream Signatures (BSS) を使用します。アプリケーションの動作が Behavior Stream Signatures (BSS) に一致すると、Kaspersky Endpoint Security は選択した応答処理を実行します。Behavior Stream Signatures (BSS) に基づいた Kaspersky Endpoint Security の機能は、コンピュータでプロアクティブディフェンスを可能とします。

既定では、ふるまい検知が有効になっており、カスペルスキーのエキスパートが推奨するモードで実行されます。必要に応じて、ふるまい検知を無効にすることができます。

[Web コンソールを使用してふるまい検知を有効または無効にする](#)

1. Web コンソールのメインウィンドウで、[アセット (デバイス)] → [ポリシーとプロファイル] の順に選択します。

2. Kaspersky Endpoint Security ポリシーの名前をクリックします。

ポリシーのプロパティウィンドウが表示されます。

3. [アプリケーション設定] タブを選択します。

4. [先進の脅威対策] → [ふるまい検知] の順に移動します。

5. [ふるまい検知] スイッチをオンまたはオフにします。

6. ふるまい検知をオンにする場合、マルウェアの活動の検知時に実行する処理を次から洗濯します：

- [ブロック](#)

このオプションをオンにすると、悪意のある活動の検知時に、アプリケーションが終了されます。

- [削除](#)

このオプションをオンにすると、悪意のある活動の検知時に、悪意のあるアプリケーションの実行ファイルが削除されて、そのファイルのバックアップコピーがバックアップに作成されます。

- [手動選択](#)

このオプションをオンにすると、マルウェア活動の検知時に、悪意のあるオブジェクトに関する情報が通知ウィンドウに表示されて、Kaspersky Endpoint Security が実行する処理を選択するようユーザーに要求します。実行可能な処理は、オブジェクトの状態によって異なる場合があります。

7. ふるまい検知と外部からの暗号化に対する共有フォルダーの保護が有効になっている場合は、外部からの暗号化の検知時に実行する次のいずれかの処理を選択します：

- [通知する](#)

このオプションをオンにした場合、共有フォルダーにあるファイルを変更する試行が検知されると、この試行に関する情報がアクティブな脅威のリストに追加され、ローカルの製品レポートに項目が追加されて、検知された悪意のある活動に関する情報が Kaspersky Security Center に送信されます。

- [攻撃元コンピュータをブロックする期間](#)

このオプションをオンにした場合、共有フォルダーにあるファイルを変更する試行が検知されると、悪意のある活動を開始したセッションのファイル変更に対するアクセスがブロック（読み取り専用に変更）され、変更されたファイルのバックアップコピーが作成されます。

8. 変更を保存します。

[管理コンソールを使用してふるまい検知を有効または無効にする](#)

1. 管理コンソールを起動します。

2. [管理サーバ - <サーバ名>] フォルダを展開します。

3. コンソールツリーで、[管理対象デバイス] をクリックします。

4. 作業領域で、[ポリシー] タブを選択します。

5. 設定するポリシーを右クリックして **プロパティ** を選択します。
6. **プロパティ** ウィンドウで、**先進の脅威対策** → **ふるまい検知** の順に選択します。
7. **ふるまい検知** をオンまたはオフにします。
8. 必要に応じて、**マルウェア活動の検知時の処理** セクションで、マルウェア活動の検知時に実行する処理を選択します。
9. **[OK]** をクリックして変更を保存します。
10. 次のいずれかを選択し、ポリシーに変更を適用します：
 - **[適用]** をクリックし、**ポリシーのプロパティ** ウィンドウが開いたままの状態に変更を保存します。
 - **[OK]** をクリックし、変更を保存して**ポリシーのプロパティ** ウィンドウを閉じます。

Kaspersky Endpoint Security を使用してふるまい検知を有効または無効にする

1. メニューバーで製品アイコンをクリックし、**設定** を選択します。
本製品の設定ウィンドウが表示されます。
2. **[詳細]** タブの **ふるまい検知** セクションで、**ふるまい検知を有効にする** をオンまたはオフにします。
3. **ふるまい検知を有効にする** オンにする場合は、マルウェア活動の検知時に実行する処理を次から選択します：

- **ブロック**

このオプションをオンにすると、悪意のある活動の検知時に、アプリケーションが終了されます。

- **削除**

このオプションをオンにすると、悪意のある活動の検知時に、悪意のあるアプリケーションの実行ファイルが削除されて、そのファイルのバックアップコピーがバックアップに作成されます。

- **手動選択**

このオプションをオンにすると、マルウェア活動の検知時に、悪意のあるオブジェクトに関する情報が通知ウィンドウに表示されて、Kaspersky Endpoint Security が実行する処理を選択するようユーザーに要求します。実行可能な処理は、オブジェクトの状態によって異なる場合があります。

その結果、ふるまい検知が有効になっている場合、Behavior Stream Signatures (BSS) を使用して、オペレーティングシステム内のアプリケーションの活動が分析されます。

重要：ふるまい検知を無効にすると保護コンポーネントの有効性が低下するため、絶対に必要な場合を除き、ふるまい検知は有効にしておくことを推奨します。脅威を検知するために、保護コンポーネントはふるまい検知コンポーネントによって収集されたデータを要求する場合があります。

スキャン

[ファイル脅威対策](#)や[ウェブ脅威対策](#)によるコンピュータのリアルタイム保護に加え、マルウェアやその他のコンピュータのセキュリティの脅威がないか、コンピュータを定期的にスキャンしてください。コンピュータのスキャン実行は、保護コンポーネントによって検知されなかったマルウェアの拡散を防ぐために必要です。

Kaspersky Endpoint Security には、次のスキャンタスクが組み込まれています：

-  **完全スキャン：**
コンピュータのメモリ、スタートアップオブジェクト、コンピュータのすべての内部ディスクをスキャンします。
-  **簡易スキャン：**
コンピュータの重要領域（メモリ、スタートアップオブジェクト、システムフォルダ）のみをスキャンします。
-  **オブジェクトスキャン：**
指定されたオブジェクト（ファイル、フォルダ、内部ディスク、リムーバブルディスク）をスキャンします。

• 外部ディスクのスキャン

外部ディスクがコンピュータに接続された時に、外部ディスクに対してマルウェアスキャンを実行します。

アプリケーションがスキャンタスクを実行すると、シグネチャ分析を介して悪意のあるオブジェクトが認識されます。シグネチャ分析に加え、ヒューリスティック分析やその他のスキャン技術も使用します。

「**スキャン**」ウィンドウには、実行中の各スキャンタスクの進行状況（完了率と残り時間）とスキャン履歴（最新の100件のスキャンタスク）に関する情報が表示されます。

完全スキャンと簡易スキャンを開始する

1. 本製品の**メインウィンドウ**のサイドバーで、「**スキャン**」をクリックします。
「**スキャン**」ウィンドウが表示されます。
2. 「**スキャン**」ウィンドウで、「**完全スキャン**」または「**簡易スキャン**」をクリックします。
スキャンタスクが開始されます。

オブジェクトスキャンを開始する

1. 本製品の**メインウィンドウ**のサイドバーで、「**スキャン**」をクリックします。
「**スキャン**」ウィンドウが表示されます。
2. 「**オブジェクトスキャン**」を開始するには、次のいずれかの操作を実行します。
 - ファイルまたはフォルダをウィンドウにドラッグします。
 - 「**選択**」をクリックしてファイルまたはフォルダを開きます。スキャンタスクが開始されます。

スキャンタスクを停止する

1. 本製品の**メインウィンドウ**のサイドバーで、「**スキャン**」をクリックします。
「**スキャン**」ウィンドウが表示されます。
2. 「**スキャン**」ウィンドウで、停止するスキャンの隣にある「**停止**」ボタン（)をクリックします。
確認ダイアログが開きます。
3. 確認ダイアログで、「**停止**」をクリックします。
スキャンタスクが停止します。

完全スキャンタスクまたは簡易スキャンタスクをスケジュールできます。

「スキャン」ウィンドウからスキャンタスクをスケジュールする

1. 本製品の**メインウィンドウ**のサイドバーで、「**スキャン**」をクリックします。
「**スキャン**」ウィンドウが表示されます。
2. 「**スキャンをスケジュールする**」をクリックします。
スケジュールを設定するダイアログが開きます。
3. 「**完全スキャン**」または「**簡易スキャン**」をオンにします。
4. スキャンを開始する頻度と開始時刻を指定します。
5. 「**OK**」をクリックします。

「設定」ウィンドウからスキャンタスクをスケジュールする

1. メニューバーで製品アイコンをクリックし、**〔設定〕** を選択します。
本製品の設定ウィンドウが表示されます。
2. **〔スキャン〕** タブで、**〔スケジュール〕** をクリックします。
3. 表示されるウィンドウで、スケジュールを設定して開始させるスキャンの名前の隣のチェックボックスをオンにします。
4. スキャンタスクの頻度と日時を設定します。
5. **〔OK〕** をクリックして、スキャンタスクのスケジュールの変更内容を保存します。

外部ディスクがコンピュータに接続されると、Kaspersky Endpoint Security は自動的にディスクのスキャンを開始するか、スキャンを要求するメッセージを表示するか、何もしません。外部ディスクのスキャンタスクの設定で、いずれかのオプションを選択できます。

外部ディスクがコンピュータに接続された時に、Kaspersky Endpoint Security が実行する動作を選択する

1. メニューバーで製品アイコンをクリックし、**〔設定〕** を選択します。
本製品の設定ウィンドウが表示されます。
2. **〔スキャン〕** タブの左側にあるリストから、**〔外部ディスクのスキャン〕** タスクを選択します。
3. **〔外部ディスクの接続時〕** セクションで、外部ディスクの接続時に本製品が実行する動作を選択します。

完全スキャンおよび簡易スキャンのタスクには、スキャン範囲は既に含まれています。完全スキャンタスクでは、コンピュータのメモリ、スタートアップオブジェクト、およびすべての内部ディスクをスキャンします。簡易スキャンタスクでは、コンピュータのメモリ、スタートアップオブジェクト、システムフォルダをスキャンします。簡易スキャンのスキャン範囲は変更することができます。

ご注意：読み取り専用のシステムボリュームのスキャンをスキップして、スキャン時間を大幅に短縮することができます。既定では、読み取り専用のシステムボリュームは簡易スキャンの実行時はスキャンされず、完全スキャンの実行時はスキャンされます。

注意：Kaspersky Endpoint Security は、OneDrive や iCloud ストレージ、その他のクラウドストレージにあるファイルをスキャンしません。これらのファイルをスキャン範囲から除外してください。そうしないと、スキャンタスクが「感染したファイルが削除されませんでした」というエラーで終了する可能性があります。

読み取り専用のシステムボリュームのスキャンを有効または無効にする

1. メニューバーで製品アイコンをクリックし、**〔設定〕** を選択します。
本製品の設定ウィンドウが表示されます。
2. **〔スキャン〕** タブの左側にあるリストから、**〔完全スキャン〕** または **〔簡易スキャン〕** タスクを選択します。
3. **〔最適化〕** セクションで、**〔読み取り専用のシステムボリュームのスキャンをスキップする〕** をオンまたはオフにします。

重要：最適化の操作が、セキュリティ上の理由から無効化される場合があります。

ファイルやフォルダを簡易スキャン範囲に追加または簡易スキャン範囲から削除する

1. メニューバーで製品アイコンをクリックし、**〔設定〕** を選択します。
本製品の設定ウィンドウが表示されます。
2. **〔スキャン〕** タブの左側にあるリストから、**〔簡易スキャン〕** タスクを選択します。
3. **〔スキャン範囲〕** セクションにある **〔編集〕** をクリックします。
ウィンドウが開き、簡易スキャンの範囲のオブジェクトのリストが表示されます。
4. スキャン範囲オブジェクトのリストを編集する：

- スキャン範囲にファイルまたはフォルダを追加するには：
 - a. **+** をクリックします。
ポップアップメニューが表示されます。ここから、スキャン範囲に追加するオブジェクトを選択することができます。
 - b. **〔ファイルとフォルダ〕** を選択します。
ダイアログが表示されます。ここから、ファイルまたはフォルダを選択することができます。
 - c. 簡易スキャンのスキャン範囲に追加するファイルまたはフォルダを選択します。
 - d. **〔開く〕** をクリックします。
 - 簡易スキャンの範囲からファイルやフォルダを削除するには：
 - a. 削除したいオブジェクトを選択します。
 - b. 選択したオブジェクトをウインドウからドラッグするか、**−** をクリックします。
5. **〔保存〕** をクリックします。

簡易スキャンの既定のリスト中のスキャン範囲にオブジェクトを追加する

1. メニューバーで製品アイコンをクリックし、**〔設定〕** を選択します。
本製品の設定ウインドウが表示されます。
2. **〔スキャン〕** タブの左側にあるリストから、**〔簡易スキャン〕** タスクを選択します。
3. **〔スキャン範囲〕** セクションにある **〔編集〕** をクリックします。
ウインドウが開き、スキャン範囲のオブジェクトのリストが表示されます。
4. **+** をクリックします。
ポップアップメニューが表示されます。ここから、スキャン範囲に追加するオブジェクトを選択することができます。
5. ポップアップメニューで、スキャン範囲に追加したいオブジェクト（たとえば、**〔メモリ〕**）を選択します。
6. **〔OK〕** をクリックします。

簡易スキャンのスキャン対象オブジェクトの保護を無効にする

1. メニューバーで製品アイコンをクリックし、**〔設定〕** を選択します。
本製品の設定ウインドウが表示されます。
2. **〔スキャン〕** タブの左側にあるリストから、**〔簡易スキャン〕** タスクを選択します。
3. **〔スキャン範囲〕** セクションにある **〔編集〕** をクリックします。
ウインドウが開き、スキャン範囲のオブジェクトのリストが表示されます。
4. スキャン範囲に含まれるオブジェクトのリストで、目的のオブジェクトに隣接するチェックボックスをオフにします。
5. **〔OK〕** をクリックします。

ファイル中に脅威が検知された場合、通知が表示され、指定した処理がオブジェクトに対して実行されます。オブジェクトの検知時に実行する処理を変更することができます。

感染したオブジェクトの検知時に実行する処理を指定する

1. メニューバーで製品アイコンをクリックし、**〔設定〕** を選択します。
本製品の設定ウインドウが表示されます。
2. **〔スキャン〕** タブで、タスクのリストからタスクを選択します。
3. **〔処理〕** セクションでは、感染したオブジェクトの検知時に実行する処理を選択できます。

感染したファイルを駆除または削除する前に、そのファイルのコピーがバックアップに保存されるので、必要に応じて元のファイルを復元できます。

スキャンの実行結果およびすべての検知した脅威の情報は、レポートに記録されます。

注意：マルウェアスキャンタスクの実行中にエラーが発生した場合は、そのタスクを再度実行してください。スキャンを再実行してもエラーが発生する場合は、テクニカルサポートまでお問い合わせください。

スキャンのレポートの表示

1. メニューバーで **［プロテクション］** → **［レポート］** の順に選択します。
［レポート］ ウィンドウが表示されます。
2. **［スキャン］** タブを開きます。

アップデートタスク

定義データベースを適切にアップデートすることで、コンピュータが保護された状態を維持できます。[ファイル脅威対策](#)、[ウェブ脅威対策](#)、および[スキャン](#)の各タスクでは、定義データベースを使用して、コンピュータ上のマルウェアを検知し、無害化します。定義データベースは定期的にアップデートされ、様々な種類の脅威とそれらを除去する方法が追加されます。そのため、定義データベースの定期的なアップデートは重要です。

カスペルスキーのアップデートサーバから定義データベースとソフトウェアモジュールがダウンロードされ、コンピュータにインストールされます。ディストリビューションポイント、ローカルフォルダおよびその他の **Web** サーバを使用することもできます。

注意：アップデートサーバへの接続とアップデートのダウンロードにはインターネット接続が必要です。プロキシサーバを使用してインターネットに接続する場合は、ネットワーク設定が必要になることがあります。

定義データベースのアップデートは、次のいずれかの方法でダウンロードできます：

- **自動：**カスペルスキーのアップデートサーバにあるアップデートが定期的に確認されます。新しいアップデートがサーバにある場合は、バックグラウンドでダウンロードされ、お使いのコンピュータにインストールされます。既定では、このオプションがオンです。
- **手動：**アップデートを任意の時間に手動で確認できます。

定義データベースの自動アップデートを有効または無効にする

1. メニューバーで製品アイコンをクリックし、**［設定］** を選択します。
本製品の設定ウィンドウが表示されます。
2. **［アップデート］** タブの **［定義データベース］** セクションで **［自動的にアップデートをダウンロードする］** をオンまたはオフにします。

定義データベースのアップデートを確認する

1. 本製品の[メインウィンドウ](#)のサイドバーで、**［アップデート］** をクリックします。
［アップデート］ ウィンドウが表示されます。
2. **［アップデート］** をクリックします。
定義データベースのアップデートが開始されます。

次のいずれかの方法でもアップデートタスクを開始できます。

- 製品アイコンをクリックし、**［アップデート］** を選択します。
- メニューバーで **［プロテクション］** → **［アップデート］** の順に選択します。

アップデート中、定義データベースとソフトウェアモジュールが、アップデート元にある最新のバージョンと比較されます。最新バージョンの定義データベースがコンピュータにインストールされている場合は、定義データベースが最新の状態であるというメッセージが **［アップデート］** ウィンドウに表示されます。ソフトウェアモジュールと定義データベースがアップデート元の最新のものと異なる場合は、アップデートファイルの差分のみがコンピュータにダウンロードされ、インストールされます。定義データベースの差分アップデートは時間がそれほどかからず、必要な **Web** トラフィック量も少なくなります。

プロキシサーバを経由してインターネットに接続する場合は、プロキシサーバ接続の設定を指定します。この設定は、定義データベースのアップデートやソフトウェアモジュールのアップデートをダウンロードする時に使用されます。

[プロキシサーバへの接続を設定する](#)

1. メニューバーで製品アイコンをクリックし、**「設定」** を選択します。
本製品の設定ウインドウが表示されます。
2. **「アップデート」** タブを選択します。
3. **「プロキシ」** セクションの **「プロキシサーバを使用する」** をオンにし、**「設定」** をクリックします。
ウインドウが表示され、プロキシサーバ接続の設定を指定できます。
4. プロキシサーバへの接続を設定します。
5. **「保存」** をクリックして、プロキシサーバ接続の設定に対する変更内容を保存します。

ロールバックが必要となる場合に備え、定義データベースのアップデート前にバックアップコピーが作成されます。ロールバック機能は、新しいバージョンの定義データベースに正しくないシグネチャが存在することが原因で、Kaspersky Endpoint Security が安全なアプリケーションをブロックする場合などに役立ちます。

注意： 定義データベースが破損した場合は、[アップデートを開始](#)して最新の定義データベースをダウンロードし、インストールしてください。

[前回のアップデートのロールバック](#)

1. メニューバーで製品アイコンをクリックし、**「設定」** を選択します。
本製品の設定ウインドウが表示されます。
2. **「アップデート」** タブを選択します。
3. **「ロールバック」** セクションで、**「アップデートのロールバック」** をクリックします。

Kaspersky Endpoint Security では、**「レポート」** ウインドウにアップデートの実行結果についての詳細レポートも表示されます。

[アップデートタスクのレポートを表示する](#)

1. メニューバーで **「プロテクション」** → **「レポート」** の順に選択します。
2. **「レポート」** ウインドウが表示されます。
3. **「アップデート」** タブを開きます。

ご注意： アップデート機能（マルウェア対策の署名のアップデートおよびコードベースのアップデートの提供を含む）および KSN 機能は、アメリカ合衆国内にある本ソフトウェアではご利用いただけなくなる可能性があります。

ローカルタスク

外部ディスクのスキャンタスク

Kaspersky Endpoint Security は、ファイルが外部ディスク上にある場合でも、実行またはコピーするすべてのファイルをスキャンできます。マルウェアの拡散を防ぐために、外部ディスクのデバイスへの接続時に自動的にスキャンするように設定できます。

外部ディスクスキャンに対して次の設定を指定できます：

- [外部ディスクの接続時にKaspersky Endpoint Security が実行する動作。](#)

[スキャン](#)

このオプションをオンにすると、Kaspersky Endpoint Security は接続された外部ディスクのマルウェアスキャンタスクを開始します。

既定では、このオプションがオンです。

[何もしない](#)

このオプションをオンにすると、Kaspersky Endpoint Security は接続された外部ディスクをスキャンしません。

• [悪意のあるオブジェクトの検知時に Kaspersky Endpoint Security が実行する処理を指定します。](#)

[駆除する。駆除できない場合は削除する](#)

このオプションをオンにすると、感染したファイルへのアクセスをブロックし、ユーザの確認を要求せずにファイルを自動的に駆除します。

オブジェクトが駆除されると、元の保存場所に元のファイル名で保存されます。駆除に失敗した場合、駆除できなかった感染オブジェクトが削除されます。

既定では、このオプションがオンです。

[手動選択](#)

このオプションをオンにすると、悪意のあるオブジェクトに関する情報を含む通知ウィンドウが表示され、Kaspersky Endpoint Security が実行する処理をユーザが選択するよう要求されるようになります。実行可能な処理は、オブジェクトの状態によって異なる場合があります。

外部ディスクスキャンは、管理コンソール、Web コンソール、または Kaspersky Endpoint Security で設定できます。

[管理コンソール（MMC）で外部ディスクスキャンを設定する方法](#)

1. Kaspersky Security Center の管理コンソールを起動します。
2. [管理サーバ - <サーバ名>] フォルダを展開します。
3. コンソールツリーで、[管理対象デバイス] をクリックします。
4. 作業領域で、[ポリシー] タブを選択します。
5. 設定するポリシーを右クリックして [プロパティ] を選択します。
6. [プロパティ] ウィンドウで、[ローカルタスク] → [外部ディスクのスキャン] の順に選択します。
7. スキャンタスクの設定を編集します。
8. [OK] をクリックして変更を保存します。

[Web コンソールと Cloud コンソールで外部ディスクスキャンの実行を設定する方法](#)

1. Web コンソールのメインウィンドウで、[デバイス] → [ポリシーとプロファイル] の順に選択します。
2. Kaspersky Endpoint Security ポリシーの名前をクリックします。
ポリシーのプロパティウィンドウが表示されます。
3. [アプリケーション設定] タブを選択します。
4. [ローカルタスク] → [外部ディスクのスキャン] の順に選択します。
5. スキャンタスクの設定を編集します。
6. [OK] をクリックして変更を保存します。

本製品のインターフェイスで外部ディスクのスキャンの実行を設定する方法 ②

1. メニューバーで製品アイコンをクリックし、**「設定」** を選択します。
本製品の設定ウインドウが表示されます。
2. **「スキャン」** タブの左側にあるリストから、**「外部ディスクのスキャン」** タスクを選択します。
3. **「外部ディスクの接続時」** セクションで、外部ディスクの接続時に本製品が実行する動作を選択します。

バックアップ

感染したファイルの駆除の実行中に、そのファイルの完全性を維持できないことがあります。駆除後にファイルの一部または全部にアクセスできない場合は、バックアップから元のファイルを復元できます。

「バックアップコピー」とは、ファイルを駆除または削除した時に作成された、危険なファイルのコピーです。バックアップコピーはバックアップに保存されます。

「バックアップ」とは、駆除の過程で削除または変更されたファイルのバックアップコピーを保存する、特別な保管領域です。バックアップの主な機能は、ユーザが元のファイルをいつでも復元できるようにすることです。バックアップ内のファイルは特別な形式で保存されているため、コンピュータに対する危険性はありません。

バックアップの内容を確認する ②

1. メニューバーで **「プロテクション」** → **「検知したオブジェクト」** の順に選択します。
「検知したオブジェクト」 ウインドウが開きます。
2. **「バックアップ」** セクションには、バックアップされたファイルのリストが表示されます。

バックアップからファイルのバックアップコピーを復元または削除できます。

バックアップからファイルのバックアップコピーを復元する ②

1. メニューバーで **「プロテクション」** → **「検知したオブジェクト」** の順に選択します。
「検知したオブジェクト」 ウインドウが開きます。
2. **「バックアップ」** セクションで、復元するファイルに隣接する ******* をクリックします。
ポップアップメニューが表示されます。
3. **「ファイルを復元」** を選択します。
ファイル名、タグ、ファイルの復元先フォルダを指定するウインドウが表示されます。既定では、元のファイル名と元の保存場所があらかじめ指定されています。
4. ファイル名とファイルの復元先のフォルダを指定します。
5. **「保存」** をクリックします。

ファイルは指定された場所に指定された名前で復元されます。

復元後には、すぐにファイルのマルウェアスキャンを実行してください。アップデートされた定義データベースでスキャンすることで、オブジェクトを破損させずに駆除できる可能性があります。

重要：コンピュータが感染する可能性があるため、どうしても必要である場合を除き、バックアップコピーからファイルを復元しないでください。

バックアップからファイルのバックアップコピーを削除する ②

1. メニューバーで **「プロテクション」** → **「検知したオブジェクト」** の順に選択します。
「検知したオブジェクト」 ウインドウが開きます。

2. **「バックアップ」** セクションで、次の操作を実行します：

- すべてのバックアップコピーを削除するには、**「すべて削除」** をクリックします。
- バックアップコピーを選択して削除するには、バックアップコピーの隣の ******* をクリックし、**「バックアップコピーを削除」** を選択します。

既定では、バックアップにあるファイルの保存期間は **30** 日です。この期間を過ぎると、ファイルは削除されます。ファイルの隔離内の保存期間を変更したり、保存期間の制限を解除したりできます。

[バックアップにファイルを保存する期間を設定する](#)

- メニューバーで製品アイコンをクリックし、**「設定」** を選択します。
本製品の設定ウインドウが表示されます。
- 「脅威」** タブの **「バックアップ」** セクションで、**「オブジェクトを削除するまでの期間」** をオンにし、バックアップに保管されているファイルを自動的に削除するまでの期間を指定します。

レポート

検知された全オブジェクトがリストされた **Kaspersky Endpoint Security** レポートが、**「処理されたオブジェクト」** タブに表示されます。システムイベントは、**「システムイベント」** タブに表示されます。また、次のコンポーネントごとの詳細レポートが作成されます：[ファイル脅威対策](#)、[ウェブ脅威対策](#)、[ネットワーク脅威対策](#)、[ふるまい検知](#)、[スキャンタスク](#)と[アップデートタスク](#)。

[「レポート」ウインドウを表示する](#)

メニューバーで **「プロテクション」** → **「レポート」** の順に選択します。

レポートをテキスト形式で保存できます。この機能は、製品コンポーネントまたはタスクでエラーが発生し、ご自身での解決ができず、カスペルスキーのテクニカルサポートによるサポートが必要である場合に役立ちます。この場合、テクニカルサポートにテキストレポートを送信して、できるだけ速やかに問題を詳しく調査し、解決できるようにします。

[本製品のコンポーネントまたはタスクのレポートをテキストファイルにエクスポートする](#)

- メニューバーで **「プロテクション」** → **「レポート」** の順に選択します。
「レポート」 ウインドウが表示されます。
- 左ペインで、目的のレポートタブを選択します。
- 右上部の  をクリックします。
- 表示されたウインドウに、レポートのファイル名、タグ、保存先フォルダを指定します。
- 「保存」** をクリックします。

既定では、レポートに情報イベントは記録されません。情報イベントの記録は、有効にすることができます。

[情報イベントのレポートへの記録を有効にする](#)

- メニューバーで製品アイコンをクリックし、**「設定」** を選択します。
本製品の設定ウインドウが表示されます。
- 「インターフェイス」** タブの **「レポート」** セクションで、**「緊急イベント以外も記録する」** をオンにして、本製品の情報に関する通知を受信します。

Managed Detection and Response

Managed Detection and Response コンポーネントが、**Kaspersky Endpoint Security** バージョン 11.2 に追加されました。このコンポーネントは、**Kaspersky Managed Detection and Response** として知られるソリューションと対話します。*Kaspersky Managed Detection and Response (MDR)* は、組織を標的とする脅威を継続的に探索、検知、排除します。ソリューションの動作の詳細は、[Kaspersky Managed Detection and Response のヘルプ](#)を参照してください。

Kaspersky Managed Detection and Response との対話時に、本製品が実行可能な機能は次の通りです：

- Managed Detection and Response の有効化。BLOB 設定情報ファイルを使用します。
- Kaspersky Managed Detection and Response からのコマンドの実行。
- 脅威の検知を目的とした、テレメトリデータを Kaspersky Managed Detection and Response へ送信。

Managed Detection and Response には次の追加要件があります：

- macOS 12 以降
- Intel ベースの Mac、Apple シリコン
- Kaspersky Endpoint Security の現在のライセンス

Kaspersky Managed Detection and Response との統合

Kaspersky Managed Detection and Response との連携は、次のステップで構成されます：

1 Kaspersky Security Network プロキシサーバの設定

Kaspersky Security Network プロキシサーバが、コンピュータと Kaspersky Security Network クラウドサービスインフラストラクチャ間のデータ交換を支援します。直接のデータ交換の代わりに、管理サーバーの仲介を使用します。

Kaspersky Security Network 設定情報ファイルを、管理サーバーのプロパティで読み込みます。Kaspersky Security Network 設定情報ファイルは、ZIP アーカイブファイル内か、MDR 設定情報ファイルのアーカイブファイル内にあります。ZIP アーカイブファイルは、Kaspersky Managed Detection and Response コンソールで入手可能です。Kaspersky Security Network プロキシサーバの設定の詳細は、[Kaspersky Security Center のヘルプ](#) を参照してください。

これにより、Kaspersky Endpoint Security はプライベート KSN を使用して、ファイル、アプリケーション、Web サイトの評価を決定するようになります。動作ステータス「インフラストラクチャ：Kaspersky Private Security Network」が、ポリシー設定の「Kaspersky Security Network」セクションで指定されます。

プライベート KSN を Kaspersky Managed Detection and Response とともに使用することで、GDPR（General Data Protection Regulation）を遵守するサーバへデータが送信されます。プライベート KSN を使用しない場合は、グローバル KSN へテレメトリが送信される可能性があります。お住まいの地域によっては、法的に違反する場合があります。

重要： [拡張 KSN モードを有効](#) にして、Managed Detection and Response を動作させる必要があります。

2 Managed Detection and Response の有効化

Kaspersky Endpoint Security のポリシーで BLOB 設定ファイルを読み込みます（下の手順を参照してください）。BLOB ファイルには、クライアント ID および Kaspersky Managed Detection and Response のライセンスに関する情報が含まれます。BLOB ファイルは、ZIP アーカイブファイル内か、MDR 設定情報ファイルのアーカイブファイル内にあります。ZIP アーカイブファイルは、Kaspersky Managed Detection and Response コンソールで入手可能です。BLOB ファイルの詳細は、[Kaspersky Managed Detection and Response のヘルプ](#) を参照してください。

[Managed Detection and Response を管理コンソール \(MMC\)で有効化します](#)

1. Kaspersky Security Center の管理コンソールを起動します。
2. [管理サーバ - <サーバ名>] フォルダを展開します。
3. コンソールツリーで、[管理対象デバイス] をクリックします。
4. 作業領域で、[ポリシー] タブを選択します。
5. 設定するポリシーを右クリックして [プロパティ] を選択します。
6. [プロパティ] ウィンドウで、[Detection and Response] → [Managed Detection and Response] の順に選択します。
7. [Managed Detection and Response] をオンにします。
8. [MDR 設定情報ファイル] セクションで [インポート] をクリックし、Kaspersky Managed Detection and Response コンソールで取得した BLOB ファイルを選択します。このファイルの拡張子は、.P7 です。
9. [OK] をクリックして変更を保存します。

[Managed Detection and Response を、Web コンソール、Cloud コンソールで有効化します](#)

1. Web コンソールのメインウィンドウで、[デバイス] → [ポリシーとプロファイル] の順に選択します。
2. Kaspersky Endpoint Security for Mac ポリシーの名前をクリックします。
3. ポリシーのプロパティウィンドウが表示されます。
4. [アプリケーション設定] タブを選択します。
5. [Detection and Response] → [Managed Detection and Response] の順に選択します。
6. [Managed Detection and Response] のスイッチをオンにします。
7. [インポート] をクリックし、Kaspersky Managed Detection and Response コンソールで取得した BLOB ファイルを選択します。このファイルの拡張子は、.P7 です。
8. 変更を保存します。

これにより、BLOB ファイルが検証されます。BLOB ファイルの検証中に、デジタル署名とライセンス条項もチェックされます。BLOB ファイルが検証されると、ファイルが読み取られ、Kaspersky Security Center との次の同期中にファイルがコンピュータに送信されます。

Endpoint Detection and Response (KATA)

Kaspersky Endpoint Security は、Kaspersky Anti Targeted Attack Platform ソリューションの一部として、Kaspersky Endpoint Detection and Response コンポーネントとの統合をサポートします。このソリューションは、標的型攻撃、高度な持続的脅威、ゼロデイ攻撃などの高度な脅威を迅速に検知する目的で設計されています。ソリューションの動作の詳細は、[Kaspersky Anti Targeted Attack Platform のヘルプ](#) を参照してください。

Endpoint Detection and Response (KATA) との統合が設定されている場合、KATA サーバーは、Kaspersky Endpoint Security の動作中に発生するイベント、検知された脅威に関する情報、およびこれらの脅威の処理に関する情報を受信します。検知された脅威に対応するために、Kaspersky Endpoint Security は、Kaspersky Anti Targeted Attack Platform Web インターフェイスで開始されたタスクを実行する場合があります。

Endpoint Detection and Response (KATA) には、次の追加要件があります：

- Kaspersky Anti Targeted Attack Platform 6.0 以降。
- Kaspersky Security Center 14.2 以降。
- Endpoint Detection and Response (KATA) との統合は、Kaspersky Security Center 管理コンソール (MMC)、Web コンソール、または Cloud コンソールで設定できます。

Kaspersky Endpoint Detection and Response (KATA) との統合

Kaspersky Managed Detection and Response (KATA) との連携は、次のステップで構成されます：

1 Endpoint Detection and Response コンポーネントのインストール

Kaspersky Endpoint Security のインストール中に、Endpoint Detection and Response コンポーネントを選択できます。

2 Endpoint Detection and Response の有効化

Endpoint Detection and Response コンポーネントが現在のライセンスでサポートされていない場合は、Kaspersky Endpoint Detection and Response を個別にアクティベートする必要があります。

[ライセンス] ウィンドウで、Endpoint Detection and Response 機能が現在のライセンスでサポートされているかどうかを確認できます。

3 KATA サーバーへの接続

Kaspersky Anti Targeted Attack Platform、Kaspersky Endpoint Security と KATA サーバーの間に信頼できる接続を確立する必要があります。信頼できる接続を設定するには、TLS 証明書を使用する必要があります。TLS 証明書は、Kaspersky Anti Targeted Attack Platform Web インターフェイスでダウンロードできます。証明書のダウンロードの詳細は、[Kaspersky Anti Targeted Attack Platform のヘルプ](#) を参照してください。

既定では、Kaspersky Endpoint Security は KATA サーバーの TLS 証明書のみをチェックします。接続のセキュリティを向上させるために、相互認証を有効にすることができます。相互認証を有効にするには、パスワードで保護された暗号化コンテナを使用する必要があります。暗号化コンテナのダウンロードの詳細は、[Kaspersky Anti Targeted Attack Platform のヘルプ](#) を参照してください。

[管理コンソールを使用して、Kaspersky Endpoint Security がインストールされたコンピュータを KATA サーバーに接続する](#) 

1. 管理コンソールを起動します。
2. [管理サーバ - <サーバ名>] フォルダを展開します。
3. コンソールツリーで、[管理対象デバイス] をクリックします。

4. 作業領域で、**［ポリシー］** タブを選択します。
5. 設定するポリシーを右クリックして **［プロパティ］** を選択します。
6. **［プロパティ］** ウィンドウで、 **［Detection and Response］** → **［Endpoint Detection and Response (KATA)］** の順に選択します。
7. **［Endpoint Detection and Response (KATA)］** をオンにします。
8. **［サーバーの接続設定］** をクリックします。
9. 表示された **［サーバーの接続設定］** ウィンドウで、次の設定を指定します：
 - **［TLS 証明書を追加］** をクリックして、KATA サーバーとの信頼された接続の確立に使用される TLS 証明書を選択します。
 - KATA サーバーの応答タイムアウトを変更する場合は、 **［タイムアウト（秒）］** フィールドにタイムアウト期間を指定します。タイムアウトが経過すると、Kaspersky Endpoint Security は別の KATA サーバーへの接続を試行します。
 - 相互認証を使用する場合は、 **［相互認証を使用する］** をオンにします。**［暗号化されたコンテナを読み込む］** をクリックして暗号化コンテナファイルを選択し、パスワードを **［暗号化されたコンテナのパスワード］** フィールドに入力します。
10. **［保存］** をクリックします。
11. KATA サーバーを追加するには、 **［追加］** をクリックします。
12. 表示された **［KATA サーバー］** ウィンドウで、サーバーのアドレスとポートを指定し、**［保存］** をクリックします。
13. **［OK］** をクリックして変更を保存します。

Web コンソールを使用して、Kaspersky Endpoint Security がインストールされたコンピュータを KATA サーバーに接続する

1. Web コンソールのメインウィンドウで、**［デバイス］** → **［ポリシーとプロファイル］** の順に選択します。
2. Kaspersky Endpoint Security for Mac ポリシーの名前をクリックします。
ポリシーのプロパティウィンドウが表示されます。
3. **［アプリケーション設定］** タブを選択します。
4. **［Detection and Response］** → **［Endpoint Detection and Response (KATA)］** の順に選択します。
5. **［Endpoint Detection and Response (KATA)］** スイッチをオンにします。
6. **［サーバーの接続設定］** をクリックします。
7. 表示された **［サーバーの接続設定］** ウィンドウで、次の設定を指定します：
 - **［TLS 証明書を追加］** をクリックして、KATA サーバーとの信頼された接続の確立に使用される TLS 証明書を選択します。
 - KATA サーバーの応答タイムアウトを変更する場合は、 **［タイムアウト（秒）］** フィールドにタイムアウト期間を指定します。タイムアウトが経過すると、Kaspersky Endpoint Security は別の KATA サーバーへの接続を試行します。
 - 相互認証を使用する場合は、 **［相互認証を使用する］** をオンにします。**［暗号化されたコンテナを読み込む］** をクリックして暗号化コンテナファイルを選択し、パスワードを **［暗号化されたコンテナのパスワード］** フィールドに入力します。
8. **［OK］** をクリックします。
9. KATA サーバーを追加するには、 **［追加］** をクリックします。
10. 表示されたダイアログでサーバーのアドレスとポートを指定し、 **［OK］** をクリックします。
11. 変更を保存します。

これにより、Kaspersky Anti Targeted Attack Platform の Web インターフェースにコンピュータが表示されます。

Endpoint Detection and Response Optimum

バージョン 12.1 以降、Kaspersky Endpoint Security for Mac には、Kaspersky Endpoint Detection and Response Optimum ソリューション（以降「EDR Optimum」とも表記）のビルトインエージェントが含まれています。このソリューションは、企業の IT インフラストラクチャを高度なサイバー脅威から保護することを目的に設計されています。このソリューションの機能は、脅威の自動検知と、これらの脅威に対応する能力を組み合わせ、新種の脆弱性攻撃、ランサムウェア、ファイルレス攻撃、正規のシステムツールを使用した方法などの高度な攻撃に対抗します。このソリューションの詳細は、[Kaspersky Endpoint Detection and Response Optimum のヘルプ](#)  を参照してください。

Kaspersky Endpoint Detection and Response は、脅威の発生状況についてレビューおよび分析を行い、想定される攻撃へのタイムリーな対応に必要な情報を、セキュリティ担当者または管理者に提供します。Kaspersky Endpoint Detection and Response は、アラートの詳細を別のウィンドウに表示します。アラートの詳細は、検知された脅威に関する収集された情報全体を表示するためのツールです。アラートの詳細には、たとえば、コンピュータに表示されるファイルの履歴が含まれます。アラートの詳細を管理する方法の詳細は、[Kaspersky Endpoint Detection and Response Optimum のヘルプ](#) を参照してください。

注意：EDR Optimum コンポーネントは、Web コンソールで設定できます。

Endpoint Detection and Response の設定

パラメータ	説明
ネットワーク分離	検知された脅威に応じて、コンピュータをネットワークから自動的に分離します。 ネットワーク分離がオンになっている場合、すべてのアクティブな接続が接続され、コンピュータ上のすべての新しい TCP/IP 接続がブロックされます。次の接続のみがアクティブな状態を維持されます： - ネットワーク分離の除外リストにリストされている接続。 - Kaspersky Endpoint Security サービスによって開始された接続。 - Kaspersky Security Center ネットワーク エージェントによって開始された接続。
分離されたコンピュータのロックを自動的に解除するまでの時間（時間）	ネットワーク分離は、指定された時間後に自動的にオフにすることも、手動でオフにすることもできます。既定では、分離の開始から 8 時間後にネットワーク分離をオフにします。
ネットワーク分離の除外リスト	ネットワーク分離からの除外ルールのリスト。ネットワーク分離がオンになっている場合、ルールに一致するネットワーク接続はコンピュータ上でブロックされません。 ネットワーク分離の除外を設定するには、標準ネットワークプロファイルのリストを使用できます。既定では、除外リストには、DNS/DHCP サーバーおよび DNS/DHCP クライアントの役割を持つデバイスの中断のない動作を保証するルールを含むネットワークプロファイルが含まれます。標準ネットワークプロファイルの設定を変更したり、除外を手動で定義したりすることもできます。
重要：ポリシーのプロパティで指定された除外は、検知された脅威に応じてネットワーク分離が自動的にオンになっている場合のみ適用されます。コンピュータのプロパティで指定された除外は、Kaspersky Security Center コンソールのコンピュータのプロパティまたはアラートの詳細でネットワーク分離が手動でオンになっている場合のみ適用されます。	
実行防止	実行防止により、実行可能ファイルやスクリプトの実行の管理や、Office 形式のファイルを開くことの管理が可能です。この方法では、たとえば、セキュアでないと思われるアプリケーションの実行を防ぐことができます。これにより、脅威の拡散を阻止することができます。実行防止は、一連のスクリプトインタープリタをサポートします。 実行防止コンポーネントを使用するには、実行防止ルールを追加する必要があります。実行防止ルールは、オブジェクトの実行をブロックする場合など、オブジェクトの実行に反応する時に本製品が考慮する一連の基準です。本製品は、パスまたは MD5 および SHA256 ハッシュアルゴリズムを使用して計算されたチェックサムによってファイルを識別します。
禁止されたオブジェクトを実行、または開いたときの処理	ブロックしてレポートに書き込む：このモードでは、防止ルールの基準に一致するオブジェクトの実行や、ドキュメントを開く動作がブロックされます。オブジェクトの実行の試行やドキュメントを開こうとする動作に関するイベントも、Kaspersky Security Center のイベントログと一元化されたログ記録システムに公開されます。 イベントの記録のみ：このモードでは、Kaspersky Endpoint Security は、防止ルールの条件に一致する実行可能オブジェクトの実行やドキュメントを開こうとする動作に関するイベントを Kaspersky Security Center イベントログと一元化されたログ記録システムに公開しますが、オブジェクトまたはドキュメントの実行の試行や開こうとする動作はブロックしません。既定では、このモードがオンです。
Cloud Sandbox	Cloud Sandbox は、コンピュータ上の高度な脅威を検出する技術です。Kaspersky Endpoint Security は、検知されたファイルを分析のために Cloud Sandbox に自動的に転送します。Cloud Sandbox はこれらのファイルを隔離された環境で実行し、悪意のある活動を識別してその評価を決定します。これらのファイルのデータは、Kaspersky Security Network に送信されます。したがって、Cloud Sandbox が悪意のあるファイルを検知した場合、Kaspersky Endpoint Security は、このファイルが検知されたすべてのコンピュータでこの脅威を排除するための適切な動作を実行します。
注意：Cloud Sandbox 技術は恒常的に有効になっており、使用しているライセンス種別に関係なく、すべての Kaspersky Security Network ユーザーによる使用が可能です。	

Endpoint Detection and Response Optimum との連携

Kaspersky Endpoint Detection and Response と連携させるには、Endpoint Detection and Response Optimum（EDR Optimum）コンポーネントを追加し、Kaspersky Endpoint Security を設定する必要があります。

注意： EDR Optimum と Endpoint Detection and Response (KATA) コンポーネントは相互に互換性がありません。

Endpoint Detection and Response が機能するには、次の条件を満たす必要があります：

- Kaspersky Security Center バージョン 13.2 以降。Kaspersky Security Center の古いバージョンでは、Endpoint Detection and Response 機能を有効にすることはできません。
- Kaspersky Endpoint Detection and Response 管理プラグインがインストールされています。これは、Windows、Mac、Linux のオペレーティングシステム上でエージェントと連携するための単一のプラグインです。Endpoint Detection and Response Optimum を使用する場合、脅威へのレスポンスタスクを作成するには Kaspersky Endpoint Security 管理プラグインが必要となり、アラートの詳細を表示するには EDR 管理プラグインが必要となります。
- Kaspersky Endpoint Security の一部としての EDR Optimum コンポーネントは Kaspersky Endpoint Detection and Response Optimum 3.0 ソリューションとの連携をサポートします。Kaspersky Endpoint Detection and Response Optimum の以前のバージョンとの対話はサポートされていません。
- EDR Optimum は、Web コンソールと Cloud コンソールで管理できます。
- 本製品がアクティベートされ、ライセンスによって許可された機能が使用できます。
- Endpoint Detection and Response コンポーネントがオンになっています。

Kaspersky Endpoint Detection and Response Optimum との連携

Kaspersky Managed Detection and Response との連携は、次のステップで構成されます：

1 Endpoint Detection and Response コンポーネントのインストール

Kaspersky Endpoint Security のインストール中に、Endpoint Detection and Response コンポーネントを選択できます。

2 Endpoint Detection and Response の有効化

Endpoint Detection and Response コンポーネントが現在のライセンスでサポートされていない場合は、Kaspersky Endpoint Detection and Response を個別にアクティベートする必要があります。

[[ライセンス](#)] ウィンドウで、Endpoint Detection and Response 機能が現在のライセンスでサポートされているかどうかを確認できます。

3 Endpoint Detection and Response コンポーネントの有効化

Kaspersky Endpoint Security for Mac のポリシー設定で、コンポーネントを有効または無効にすることができます。

[Web コンソールと Cloud コンソールで Endpoint Detection and Response コンポーネントを有効または無効にする方法](#) 

1. Web コンソールのメインウィンドウで、[[アセット \(デバイス\)](#)] → [[ポリシーとプロファイル](#)] の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
ポリシーのプロパティウィンドウが表示されます。
3. [[アプリケーション設定](#)] タブを選択します。
4. [[Detection and Response](#)] → [[Endpoint Detection and Response](#)] の順に選択します。
5. [[Endpoint Detection and Response が有効です](#)] スイッチをオンにします。
6. 変更を保存します。

セキュリティ侵害インジケータのスキャン

セキュリティ侵害インジケータ (IOC) は、コンピュータへの不正アクセス（データの侵害）を示すオブジェクトまたは活動に関するデータのセットです。たとえば、システムへのサインインの試行が何度も失敗すると、セキュリティ侵害インジケータとなる可能性があります。IOC スキャンタスクを使用すると、コンピュータ上のセキュリティ侵害インジケータを検知し、脅威への対応策を講じることができます。

Kaspersky Endpoint Security は IOC ファイルを使用して侵害インジケータを検索します。IOC ファイルは、本製品が検知をカウントする目的で一致を試行するインジケータのセットを含むファイルです。IOC ファイルは、[IOC ファイルの要件](#)を満たしている必要があります。

IOC スキャンタスクの実行モード

Kaspersky Endpoint Detection and Response と、侵害されたデータを検知するための標準の IOC スキャンタスクを作成できます。標準 IOC スキャンタスクは、Web コンソールで手動で作成および設定されるグループタスクまたはローカルタスクです。タスクは、ユーザーが準備した IOC ファイルを使用して実行されます。セキュリティ侵害インジケータを手動で追加する場合は、[IOC ファイルの要件](#)をお読みください。

IOC スキャンタスクの作成

IOC スキャンタスクを手動で作成できます：

- アラートの詳細（EDR Optimum のみ）：

アラートの詳細は、検知された脅威に関する収集された情報全体を表示するためのツールです。アラートの詳細には、たとえば、コンピュータに表示されるファイルの履歴が含まれます。アラートの詳細を管理する方法の詳細は、[Kaspersky Endpoint Detection and Response Optimum のヘルプ](#) を参照してください。

- タスクウィザードの使用：

IOC スキャンタスクを作成するには：

1. Web コンソールのメインウィンドウで、**[アセット（デバイス）]** → **[タスク]** の順に選択します。

タスクのリストが開きます。

2. **[追加]** をクリックします。

新規タスクウィザードが起動します。

3. タスクの設定の編集：

a. **[アプリケーション]** ドロップダウンリストから、**[Kaspersky Endpoint Security for Mac (12.2)]** を選択します。

b. **[タスク種別]** ドロップダウン リストで、**[IOC スキャン]** を選択します。

c. **[タスク名]** フィールドに簡単な説明を入力します。

d. **タスクを割り当てるデバイスを選択する** ブロックで、タスクの範囲を選択します。

4. 選択したタスク範囲オプションに応じてデバイスを選択します。

5. **[IOC スキャン設定]** セクションで、IOC ファイルを読み込んでセキュリティ侵害インジケータを検索します。IOC ファイルを追加したり、ファイルハッシュまたは IP アドレスを含むファイルから IOC ファイルを生成することができます。

IOC ファイルの読み込み後、IOC ファイルからインジケータのリストを表示および編集できます。

注意：タスクの実行後に IOC ファイルを追加または削除することは推奨しません。これにより、タスクの以前の実行の IOC スキャン結果が誤って表示される可能性があります。新しい IOC ファイルによるセキュリティ侵害インジケータを検索するには、新しいタスクの追加を推奨します。

6. IOC 検知時の処理の設定：

- **コンピュータをネットワークから分離する：**このオプションを選択した場合、Kaspersky Endpoint Security は脅威の拡散を防ぐためにコンピュータをネットワークから分離します。[Endpoint Detection and Response コンポーネントの設定](#)で、分離の期間を設定できます。
- **コピーを隔離に移動し、オブジェクトを削除する：**このオプションを選択した場合、Kaspersky Endpoint Security はコンピュータで検知された悪意のあるオブジェクトを削除します。オブジェクトを削除する前に、後で復元する必要があった場合に備えて Kaspersky Endpoint Security はオブジェクトのバックアップコピーを作成します。Kaspersky Endpoint Security がバックアップコピーを隔離に移動します。
- **簡易スキャンを実行する：**このオプションをオンにすると、Kaspersky Endpoint Security は簡易スキャンタスクを実行します。既定では、Kaspersky Endpoint Security はメモリ、スタートアップオブジェクト、システムフォルダーをスキャンします。

7. **[詳細]** セクションに移動します。

8. タスクの一部として分析する必要があるデータ種別（IOC ドキュメント）を選択します。

注意：Kaspersky Endpoint Security は、読み込まれた IOC ファイルの内容に応じて、IOC スキャンタスクのデータ種別（IOC ドキュメント）を自動的に選択します。データ種別の選択をオフにすることは推奨されません。

さらに、次のデータ種別に対してスキャン 範囲を設定できます：

- プロセス - ProcessItem
- ファイル - FileItem
- ネットワークポート - PortItem
- ユーザーアカウント - UserItem
- ARP テーブル - ArpEntryItem

- ホスト – SystemInfoItem
- URL – UriHistoryItem
- ルート – RouteEntryItem

9. [OK] をクリックします。

10. タスクを実行するために権限を使用するユーザーのアカウント資格情報を入力します。[次へ] をクリックします。

注意：既定では、Kaspersky Endpoint Security はシステムユーザーアカウント（root）としてタスクを開始します。

11. **タスク作成の完了**手順で、[完了] をクリックしてタスクを作成し、ウィザードを閉じます。

[作成が完了したらタスクの詳細を開く] をオンにした場合は、タスク設定ウィンドウが開きます。このウィンドウでは、タスクのパラメータを確認したり、変更したり、必要に応じてタスク開始スケジュールを設定したりできます。

12. 新しいタスクをクリックします。

タスクのプロパティウィンドウが表示されます。

13. [スケジュール] タブを選択します。

14. タスクスケジュールを設定します。

注意：タスクを実行するには、コンピュータの電源がオンになっていることを確認してください。

15. [保存] をクリックします。

16. 設定したスケジュールに関係なくタスクをすぐに実行するには、次の手順を実行します：

- タスクに隣接するチェックボックスをオンにします。

17. [実行] をクリックします。

Kaspersky Endpoint Security はコンピューター上にある侵害インジケータの検索を実行します。タスクの結果は、タスクのプロパティの [結果] セクションで確認できます。検知されたセキュリティ侵害インジケータに関する情報は、タスクのプロパティ ([アプリケーション設定] → [IOC スキャン結果]) で確認できます。

注意：IOC スキャンの結果は 30 日間保存されます。この期間を経過すると、Kaspersky Endpoint Security は最も古いデータを自動的に削除します。

ファイルの隔離

[すべて表示](#) | [すべて隠す](#)

脅威に対応する際、Kaspersky Endpoint Detection and Response はファイルを隔離に移動するタスクを作成できます。これは脅威の影響を最小限に抑えるために必要です。隔離は、コンピューター上の特別なローカルの保管領域です。ユーザーは、コンピューターにとって危険であると判断したファイルを隔離できます。隔離されたファイルは暗号化された状態で保存され、デバイスのセキュリティに対する脅威となることはありません。

Kaspersky Endpoint Security は、ファイル保管先としてバックアップを使用します。ソリューションの一部として隔離を管理する方法の詳細は、[Kaspersky Endpoint Detection and Response Optimum のヘルプ](#) を参照してください。

ファイルを隔離に移動するタスクは、次の方法で作成できます：

- アラートの詳細（EDR Optimum のみ）：

アラートの詳細は、検知された脅威に関する収集された情報全体を表示するためのツールです。アラートの詳細には、たとえば、コンピューターに表示されるファイルの履歴が含まれます。アラートの詳細を管理する方法の詳細は、[Kaspersky Endpoint Detection and Response Optimum のヘルプ](#) を参照してください。

- タスクウィザードの使用：

ファイルパスまたはハッシュ（SHA256 または MD5）、またはファイルパスとファイルハッシュの両方を入力する必要があります。

ファイルを隔離に移動するタスクには次の制限があります：

- ファイルサイズは 100 MB 以内である必要があります。
- EDR Optimum のタスクは、Web コンソールで設定できます。
- バックアップ可能な容量の上限は空きディスク容量によって決定されます。

ファイルを隔離に移動するタスクを作成するには：

1. Web コンソールのメインウィンドウで、[アセット (デバイス)] → [タスク] の順に選択します。

タスクのリストが開きます。

2. [追加] をクリックします。

新規タスクウィザードが起動します。

3. タスクの設定の編集：

- a. [アプリケーション] ドロップダウンリストから、[Kaspersky Endpoint Security for Mac (12.2)] を選択します。

- b. [タスク種別] ドロップダウン リストで、 [ファイルを隔離に移動] を選択します。

- c. [タスク名] フィールドに簡単な説明を入力します。

- d. 次のいずれかのオプションを選択します：

- **管理グループにタスクを割り当てる**

タスクは管理グループに含まれるデバイスに割り当てられます。既存のグループのいずれかを指定するか、新しいグループを作成することができます。

たとえば、メッセージが特定の管理グループに含まれるデバイスに固有のものである場合、このオプションを使用して、ユーザーにメッセージを送信するタスクを実行することができます。

タスクが管理グループに割り当てられている場合、グループタスクは適用先のグループのセキュリティ設定の影響を受けるため、タスクのプロパティウィンドウに [セキュリティ] タブは表示されません。

- **デバイスのアドレスを手動で指定するか、リストからアドレスをインポートします**

タスクを割り当てるデバイスの NetBIOS 名、DNS 名、IP アドレス、IP サブネットを指定できます。

特定のサブネットに対してタスクを実行するには、このオプションを使用することができます。たとえば、経理担当者のデバイスに特定のアプリケーションをインストールしたり、感染している可能性のあるサブネット内のデバイスをスキャンしたりする場合があります。

- **デバイス抽出にタスクを割り当てる**

タスクは、デバイス抽出に含まれるデバイスに割り当てられます。既存の抽出の1つを指定できます。

たとえば、このオプションを使用して、特定のオペレーティングシステムバージョンを搭載したデバイスでタスクを実行することができます。

4. 選択したタスク範囲オプションに応じてデバイスを選択します。

5. [タスク範囲] ステップで、管理グループ、特定のアドレスを持つデバイス、またはデバイスの抽出を指定します。

使用可能な設定は、前の手順で選択したオプションによって異なります。

6. ファイルのリストで、 [追加] をクリックします。

ファイル追加ウィザードが起動します。

7. [隔離するファイルを指定してください] ドロップダウンリストで、オプションの1つを選択し、必須フィールドに入力します。ファイルを追加するには、ファイルへの完全パス、またはファイルハッシュとパスの両方を入力する必要があります。

8. タスクをシステムの重要なオブジェクトに適用できるようにする場合は、[システムの重要なオブジェクトに適用する] をオンにします。

9. タスクを実行するために権限を使用するユーザーのアカウント資格情報を入力します。[次へ] をクリックします。

注意：既定では、Kaspersky Endpoint Security はシステムユーザーアカウント (root) としてタスクを開始します。

10. タスク作成の完了手順で、 [完了] をクリックしてタスクを作成し、ウィザードを閉じます。

[作成が完了したらタスクの詳細を開く] をオンにした場合は、タスク設定ウィンドウが開きます。このウィンドウでは、タスクのパラメータを確認したり、変更したり、必要に応じてタスク開始スケジュールを設定したりできます。

11. 新しいタスクをクリックします。

タスクのプロパティウィンドウが表示されます。

12. [スケジュール] タブを選択します。

13. タスクスケジュールを設定します。

注意：タスクを実行するには、コンピュータの電源がオンになっていることを確認してください。

14. **保存** をクリックします。

15. 設定したスケジュールに関係なくタスクをすぐに実行するには、次の手順を実行します：

a. タスクに隣接するチェックボックスをオンにします。

16. **実行** をクリックします。

これにより、Kaspersky Endpoint Security はファイルを隔離領域に移動します。

現在実行中の実行可能ファイルを隔離しようとする、ファイルを隔離場所に移動するタスクがアクセス拒否エラーで終了することがあります。[プロセスの終了タスクを作成](#)して、再試行してください。

大きすぎるファイルを隔離しようとする、ファイルを隔離場所に移動するタスクが「隔離場所の保管領域に十分な空き容量がありません」というエラーで終了することがあります。ディスクの空き容量を増やしてから再試行してください。

ファイルの取得

ユーザーのコンピュータからファイルを取得できます。たとえば、サードパーティ製品によって作成されたイベントログファイルを取得するように設定できます。ファイルを取得するには、専用のタスクを作成する必要があります。タスクの実行の結果、ファイルはバックアップに保存されます。**Web** コンソールを使用して、このファイルをバックアップからコンピュータにダウンロードできます。ユーザーのコンピュータでは、ファイルは元のフォルダに残ります。

重要：ファイルサイズは 100 MB 以内にする必要があります。バックアップ可能な容量の上限は空きディスク容量によって決定されます。

ファイルの取得タスクを作成するには：

1. Web コンソールのメインウィンドウで、**アセット (デバイス)** → **タスク** の順に選択します。

タスクのリストが開きます。

2. **追加** をクリックします。

新規タスクウィザードが起動します。

3. タスクの設定の編集：

a. **アプリケーション** ドロップダウンリストから、**Kaspersky Endpoint Security for Mac (12.2)** を選択します。

b. **タスク種別** ドロップダウン リストで、**ファイルの取得** を選択します。

c. **タスク名** フィールドに簡単な説明を入力します。

d. 次のいずれかのオプションを選択します：

- **[管理グループにタスクを割り当てる](#)**

タスクは管理グループに含まれるデバイスに割り当てられます。既存のグループのいずれかを指定するか、新しいグループを作成することができます。

たとえば、メッセージが特定の管理グループに含まれるデバイスに固有のものである場合、このオプションを使用して、ユーザーにメッセージを送信するタスクを実行することができます。

タスクが管理グループに割り当てられている場合、グループタスクは適用先のグループのセキュリティ設定の影響を受けるため、タスクのプロパティウィンドウに **セキュリティ** タブは表示されません。

- **[デバイスのアドレスを手動で指定するか、リストからアドレスをインポートします](#)**

タスクを割り当てるデバイスの NetBIOS 名、DNS 名、IP アドレス、IP サブネットを指定できます。

特定のサブネットに対してタスクを実行するには、このオプションを使用することができます。たとえば、経理担当者のデバイスに特定のアプリケーションをインストールしたり、感染している可能性のあるサブネット内のデバイスをスキャンしたりする場合があります。

- **[デバイス抽出にタスクを割り当てる](#)**

タスクは、デバイス抽出に含まれるデバイスに割り当てられます。既存の抽出の1つを指定できます。
たとえば、このオプションを使用して、特定のオペレーティングシステムバージョンを搭載したデバイスでタスクを実行することができます。

4. 選択したタスク範囲オプションに応じてデバイスを選択します。[ファイルの取得] ウィンドウで、[追加] をクリックします。
[ファイルの取得] ダイアログが開きます。
5. [取得するファイルを指定してください] ドロップダウンリストで、オプションの1つを選択し、必須フィールドに入力します。
ファイルを追加するには、ファイルへの完全パス、または[ファイルハッシュ](#)とパスの両方を入力する必要があります。
6. [OK] をクリックします。
追加するファイルの設定がファイルリストに表示されます。
7. [次へ] をクリックします。
8. タスクを実行するために権限を使用するユーザーのアカウント資格情報を入力します。[次へ] をクリックします。

注意：既定では、Kaspersky Endpoint Security はシステムユーザーアカウント（root）としてタスクを開始します。

9. **タスク作成の完了**手順で、[完了] をクリックしてタスクを作成し、ウィザードを閉じます。
[作成が完了したらタスクの詳細を開く] をオンにした場合は、タスク設定ウィンドウが開きます。このウィンドウでは、タスクのパラメータを確認したり、変更したり、必要に応じてタスク開始スケジュールを設定したりできます。
10. 新しいタスクをクリックします。
タスクのプロパティウィンドウが表示されます。
11. [スケジュール] タブを選択します。
12. タスクスケジュールを設定します。

注意：タスクを実行するには、コンピュータの電源がオンになっていることを確認してください。

13. [保存] をクリックします。
14. 設定したスケジュールに関係なくタスクをすぐに実行するには、次の手順を実行します：
 - a. タスクに隣接するチェックボックスをオンにします。
15. [実行] をクリックします。
これにより、Kaspersky Endpoint Security はファイルのコピーを作成し、そのコピーをバックアップに移動します。Web コンソールのバックアップからファイルをダウンロードできます。

ファイルの削除

[すべて表示](#) | [すべて隠す](#)

ファイルの削除タスクを使用して、ファイルをリモートで削除できます。たとえば、脅威に対応する時にファイルをリモートで削除できます。

ファイルの削除タスクを作成するには：

1. Web コンソールのメインウィンドウで、[アセット（デバイス）] → [タスク] の順に選択します。
タスクのリストが開きます。
2. [追加] をクリックします。
新規タスクウィザードが起動します。
3. タスクの設定の編集：
 - a. [アプリケーション] ドロップダウンリストから、[Kaspersky Endpoint Security for Mac (12.2)] を選択します。
 - b. [タスク種別] ドロップダウン リストで、[ファイルの削除] を選択します。
 - c. [タスク名] フィールドに簡単な説明を入力します。
 - d. 次のいずれかのオプションを選択します：

- [管理グループにタスクを割り当てる](#)

タスクは管理グループに含まれるデバイスに割り当てられます。既存のグループのいずれかを指定するか、新しいグループを作成することができます。

たとえば、メッセージが特定の管理グループに含まれるデバイスに固有のものである場合、このオプションを使用して、ユーザーにメッセージを送信するタスクを実行することができます。

タスクが管理グループに割り当てられている場合、グループタスクは適用先のグループのセキュリティ設定の影響を受けるため、タスクのプロパティウインドウに **セキュリティ** タブは表示されません。

- [デバイスのアドレスを手動で指定するか、リストからアドレスをインポートします](#)

タスクを割り当てるデバイスの NetBIOS 名、DNS 名、IP アドレス、IP サブネットを指定できます。

特定のサブネットに対してタスクを実行するには、このオプションを使用することができます。たとえば、経理担当者のデバイスに特定のアプリケーションをインストールしたり、感染している可能性のあるサブネット内のデバイスをスキャンしたりする場合があります。

- [デバイス抽出にタスクを割り当てる](#)

タスクは、デバイス抽出に含まれるデバイスに割り当てられます。既存の抽出の1つを指定できます。

たとえば、このオプションを使用して、特定のオペレーティングシステムバージョンを搭載したデバイスでタスクを実行することができます。

4. 選択したタスク範囲オプションに応じてデバイスを選択します。

5. **削除するファイルを指定してください** ドロップダウンリストで、オプションの1つを選択し、必須フィールドに入力します。ファイルを追加するには、ファイルへの完全パス、またはファイルハッシュとパスの両方を入力する必要があります。

6. タスクをシステムの重要なオブジェクトに適用できるようにする場合は、**システムの重要なオブジェクトに適用する** をオンにします。

7. タスクを実行するために権限を使用するユーザーのアカウント資格情報を入力します。**次へ** をクリックします。

注意：既定では、Kaspersky Endpoint Security はシステムユーザーアカウント（root）としてタスクを開始します。

8. **タスク作成の完了** 手順で、**完了** をクリックしてタスクを作成し、ウィザードを閉じます。

作成が完了したらタスクの詳細を開く をオンにした場合は、タスク設定ウインドウが開きます。このウインドウでは、タスクのパラメータを確認したり、変更したり、必要に応じてタスク開始スケジュールを設定したりできます。

9. 新しいタスクをクリックします。

タスクのプロパティウインドウが表示されます。

10. **スケジュール** タブを選択します。

11. タスクスケジュールを設定します。

注意：タスクを実行するには、コンピュータの電源がオンになっていることを確認してください。

12. **保存** をクリックします。

13. 設定したスケジュールに関係なくタスクをすぐに実行するには、次の手順を実行します：

a. タスクに隣接するチェックボックスをオンにします。

14. **実行** をクリックします。

これにより、Kaspersky Endpoint Security はコンピュータからファイルを削除します。ファイルが別のプロセスによってロックされている場合、タスクは「完了」として表示されますが、ファイル自体はコンピュータの再起動後のみ削除されます。コンピュータを再起動した後、ファイルが削除されたことを確認します。

現在実行中の実行可能ファイルを削除しようとする、ファイルの削除タスクがアクセス拒否エラーで終了することがあります。[プロセスの終了タスクを作成](#)して、再試行してください。

プロセスを開始

プロセスの開始タスクを使用して、ファイルをリモートで実行できます。

重要：EDR Optimum のタスクは、Web コンソールで設定できます。

プロセスの開始タスクを作成するには：

1. Web コンソールのメインウィンドウで、[アセット (デバイス)] → [タスク] の順に選択します。

タスクのリストが開きます。

2. [追加] をクリックします。

新規タスクウィザードが起動します。

3. タスクの設定の編集：

a. [アプリケーション] ドロップダウンリストから、[Kaspersky Endpoint Security for Mac (12.2)] を選択します。

b. [タスク種別] ドロップダウンリストで、[プロセスを開始] を選択します。

c. [タスク名] フィールドに簡単な説明を入力します。

d. 次のいずれかのオプションを選択します：

• 管理グループにタスクを割り当てる

タスクは管理グループに含まれるデバイスに割り当てられます。既存のグループのいずれかを指定するか、新しいグループを作成することができます。

たとえば、メッセージが特定の管理グループに含まれるデバイスに固有のものである場合、このオプションを使用して、ユーザーにメッセージを送信するタスクを実行することができます。

タスクが管理グループに割り当てられている場合、グループタスクは適用先のグループのセキュリティ設定の影響を受けるため、タスクのプロパティウィンドウに [セキュリティ] タブは表示されません。

• デバイスのアドレスを手動で指定するか、リストからアドレスをインポートします

タスクを割り当てるデバイスの NetBIOS 名、DNS 名、IP アドレス、IP サブネットを指定できます。

特定のサブネットに対してタスクを実行するには、このオプションを使用することができます。たとえば、経理担当者のデバイスに特定のアプリケーションをインストールしたり、感染している可能性のあるサブネット内のデバイスをスキャンしたりする場合があります。

• デバイス抽出にタスクを割り当てる

タスクは、デバイス抽出に含まれるデバイスに割り当てられます。既存の抽出の1つを指定できます。

たとえば、このオプションを使用して、特定のオペレーティングシステムバージョンを搭載したデバイスでタスクを実行することができます。

4. 選択したタスク範囲オプションに応じてデバイスを選択します。

5. [タスク範囲] ステップで、管理グループ、特定のアドレスを持つデバイス、またはデバイスの抽出を指定します。

使用可能な設定は、前の手順で選択したオプションによって異なります。

6. タスクの設定の編集：

a. [実行コマンド] フィールドで、ローカルデバイスで実行するコマンドを指定します。

b. 必要に応じて、[コマンドライン引数 (省略可能)] フィールドにコマンドライン引数を指定します。

c. 必要に応じて、[作業フォルダーのパス (省略可能)] フィールドに実行可能ファイルへのパスを指定します。

7. タスク作成の完了手順で、[完了] をクリックしてタスクを作成し、ウィザードを閉じます。

[作成が完了したらタスクの詳細を開く] をオンにした場合は、タスク設定ウィンドウが開きます。このウィンドウでは、タスクのパラメータを確認したり、変更したり、必要に応じてタスク開始スケジュールを設定したりできます。

8. 新しいタスクをクリックします。

タスクのプロパティウィンドウが表示されます。

9. [スケジュール] タブを選択します。

10. タスクスケジュールを設定します。

注意：タスクを実行するには、コンピュータの電源がオンになっていることを確認してください。

11. **〔保存〕** をクリックします。

12. 設定したスケジュールに関係なくタスクをすぐに実行するには、次の手順を実行します：

a. タスクに隣接するチェックボックスをオンにします。

13. **〔実行〕** をクリックします。

これにより、Kaspersky Endpoint Security はサイレントモードでコマンドを実行し、プロセスを開始します。タスクの結果は、タスクのプロパティの **〔実行結果〕** セクションで確認できます。

プロセスの終了

[すべて表示](#) | [すべて隠す](#)

プロセスの終了タスクを使用して、プロセスをリモートで終了できます。たとえば、[プロセスの開始タスク](#)を使用して開始されたインターネット速度テストユーティリティをリモートで終了できます。

ファイルの実行を禁止したい場合は、[実行防止コンポーネント](#)を設定できます。実行ファイル、スクリプト、Office 形式ファイルの実行を禁止できます。

プロセスの終了タスクには次の制限があります：

- EDR Optimum のタスクは、Web コンソールでのみ設定できます。

プロセスの終了タスクを作成するには：

1. Web コンソールのメインウィンドウで、**〔アセット (デバイス)〕** → **〔タスク〕** の順に選択します。

タスクのリストが開きます。

2. **〔追加〕** をクリックします。

新規タスクウィザードが起動します。

3. タスクの設定の編集：

a. **〔アプリケーション〕** ドロップダウンリストから、**〔Kaspersky Endpoint Security for Mac (12.2)〕** を選択します。

b. **〔タスク種別〕** ドロップダウンリストで、**〔プロセスの終了〕** を選択します。

c. **〔タスク名〕** フィールドに簡単な説明を入力します。

d. 次のいずれかのオプションを選択します：

- [管理グループにタスクを割り当てる](#)

タスクは管理グループに含まれるデバイスに割り当てられます。既存のグループのいずれかを指定するか、新しいグループを作成することができます。

たとえば、メッセージが特定の管理グループに含まれるデバイスに固有のものである場合、このオプションを使用して、ユーザーにメッセージを送信するタスクを実行することができます。

タスクが管理グループに割り当てられている場合、グループタスクは適用先のグループのセキュリティ設定の影響を受けるため、タスクのプロパティウィンドウに **〔セキュリティ〕** タブは表示されません。

- [デバイスのアドレスを手動で指定するか、リストからアドレスをインポートします](#)

タスクを割り当てるデバイスの NetBIOS 名、DNS 名、IP アドレス、IP サブネットを指定できます。

特定のサブネットに対してタスクを実行するには、このオプションを使用することができます。たとえば、経理担当者のデバイスに特定のアプリケーションをインストールしたり、感染している可能性のあるサブネット内のデバイスをスキャンしたりする場合があります。

- [デバイス抽出にタスクを割り当てる](#)

タスクは、デバイス抽出に含まれるデバイスに割り当てられます。既存の抽出の1つを指定できます。

たとえば、このオプションを使用して、特定のオペレーティングシステムバージョンを搭載したデバイスでタスクを実行することができます。

4. 選択したタスク範囲オプションに応じてデバイスを選択します。

5. **「タスク範囲」** ステップで、管理グループ、特定のアドレスを持つデバイス、またはデバイスの抽出を指定します。
使用可能な設定は、前の手順で選択したオプションによって異なります。

6. ウィザードのこの手順では、**「プロセスを終了するファイルを指定してください」** ドロップダウンリストでオプションの1つを選択し、必要なフィールドに入力します。ファイルを指定するには、ファイルへの完全パス、またはファイルハッシュとパスの両方を入力する必要があります。

注意： ローカルデバイス用にこのタスクを作成する場合は、プロセスを PID で指定できます。

7. タスクをシステムの重要なオブジェクトに適用できるようにする場合は、**「システムの重要なオブジェクトに適用する」** をオンにします。

8. タスクを実行するために権限を使用するユーザーのアカウント資格情報を入力します。**「次へ」** をクリックします。

注意： 既定では、Kaspersky Endpoint Security はシステムユーザーアカウント (root) としてタスクを開始します。

9. **タスク作成の完了** 手順で、**「完了」** をクリックしてタスクを作成し、ウィザードを閉じます。

「作成が完了したらタスクの詳細を開く」 をオンにした場合は、タスク設定ウィンドウが開きます。このウィンドウでは、タスクのパラメータを確認したり、変更したり、必要に応じてタスク開始スケジュールを設定したりできます。

10. 新しいタスクをクリックします。
タスクのプロパティウィンドウが表示されます。

11. **「スケジュール」** タブを選択します。

12. タスクスケジュールを設定します。

注意： タスクを実行するには、コンピュータの電源がオンになっていることを確認してください。

13. **「保存」** をクリックします。

14. 設定したスケジュールに関係なくタスクをすぐに実行するには、次の手順を実行します：

a. タスクに隣接するチェックボックスをオンにします。

15. **「実行」** をクリックします。

これにより、Kaspersky Endpoint Security はコンピュータ上のプロセスを終了します。たとえば、ゲームアプリケーションが実行中で、ゲームプロセスを終了すると、アプリケーションはデータを保存せずに閉じられます。タスクの結果は、タスクのプロパティの **「結果」** セクションで確認できます。

実行防止

実行防止により、実行可能ファイルやスクリプトの実行の管理や、Office 形式のファイルを開くことの管理が可能です。この方法では、たとえば、セキュアでないと思われるアプリケーションの実行を防ぐことができます。これにより、脅威の拡散を阻止することができます。実行防止は、[一連のスクリプトインタープリタ](#)をサポートします。

実行防止ルール

実行防止は、実行防止ルールを使用してファイルへのユーザーアクセスを管理します。実行防止ルールは、オブジェクトの実行をブロックする場合など、オブジェクトの実行に反応する時に本製品が考慮する一連の基準です。本製品は、パスまたは MD5 および SHA256 ハッシュアルゴリズムを使用して計算されたチェックサムによってファイルを識別します。

実行防止ルールを作成できます：

- アラートの詳細 (EDR Optimum のみ)：

アラートの詳細は、検知された脅威に関する収集された情報全体を表示するためのツールです。アラートの詳細には、たとえば、コンピュータに表示されるファイルの履歴が含まれます。アラートの詳細を管理する方法の詳細は、[Kaspersky Endpoint Detection and Response Optimum のヘルプ](#) を参照してください。

- グループポリシーまたはローカルアプリケーション設定を使用する。ファイルパスまたはハッシュ (SHA256 または MD5)、またはファイルパスとファイルハッシュの両方を入力する必要があります。

[コマンドライン](#)を使用して実行防止をローカルで管理することもできます。

注意：システムの重要オブジェクト（SCO）の起動をブロックすることはできません。SCO は、オペレーティングシステムと Kaspersky Endpoint Security for Mac アプリケーションの実行に必要なファイルです。

実行防止ルールモード

実行防止コンポーネントは、次の 2 つのモードで動作します：

• 統計のみ

このモードでは、Kaspersky Endpoint Security は、防止ルールの条件に一致する実行可能オブジェクトの実行やドキュメントを開こうとする動作に関するイベントを Kaspersky Security Center イベントログと一元化されたログ記録システムに公開しますが、オブジェクトまたはドキュメントの実行の試行や開こうとする動作はブロックしません。既定では、このモードがオンです。

• アクティブ

このモードでは、防止ルールの基準に一致するオブジェクトの実行や、ドキュメントを開く動作がブロックされます。オブジェクトの実行の試行やドキュメントを開こうとする動作に関するイベントも、Kaspersky Security Center のイベントログと一元化されたログ記録システムに公開されます。

実行防止の管理

重要：コンポーネント設定は Web コンソールでのみ設定できます。

実行を防止するには：

1. Web コンソールのメインウインドウで、[デバイス] → [ポリシーとプロファイル] の順に選択します。

2. Kaspersky Endpoint Security for Mac ポリシーの名前をクリックします。

ポリシーのプロパティウインドウが表示されます。

3. [アプリケーション設定] タブを選択します。

4. [Detection and Response] → [Endpoint Detection and Response] の順に選択します。

5. [実行防止が有効です] スイッチをオンにします。

6. 禁止されたオブジェクトを実行、または開いたときの処理ブロックで、コンポーネントの動作モードを選択します：

- **ブロックしてレポートに書き込む：**このモードでは、防止ルールの基準に一致するオブジェクトの実行や、ドキュメントを開く動作がブロックされます。オブジェクトの実行の試行やドキュメントを開こうとする動作に関するイベントも、Kaspersky Security Center のイベントログと一元化されたログ記録システムに公開されます。
- **イベントの記録のみ：**このモードでは、Kaspersky Endpoint Security は、防止ルールの条件に一致する実行可能オブジェクトの実行やドキュメントを開こうとする動作に関するイベントを Kaspersky Security Center イベントログと一元化されたログ記録システムに公開しますが、オブジェクトまたはドキュメントの実行の試行や開こうとする動作はブロックしません。既定では、このモードがオンです。

7. 実行防止ルールのリストを作成します：

a. [追加] をクリックします。

b. 表示されるダイアログで、実行防止ルールの名前（たとえば、「アプリケーション A」）を入力します。

c. [種別] ドロップダウンリストで、ブロックするオブジェクト（アプリケーション、スクリプト、ドキュメント）を選択します。

オブジェクト種別を誤って選択すると、Kaspersky Endpoint Security はファイルまたはスクリプトをブロックしません。

d. ファイルを追加するには、ファイルのハッシュ（SHA256 または MD5）、ファイルへの完全パス、またはハッシュとパスの両方を入力する必要があります。

注意：ファイルがネットワークドライブ上にある場合は、次の形式でファイルパスを入力しま

す：/Volumes/shared_folder_name/filename。ファイルのパスにネットワークドライブ文字が含まれていると、Kaspersky Endpoint Security はファイルまたはスクリプトをブロックしません。

a. [OK] をクリックします。

8. 変更を保存します。

この結果、Kaspersky Endpoint Security はオブジェクトの実行（実行ファイルやスクリプトの実行、Office 形式のファイルを開く動作）をブロックします。ただし、たとえば、スクリプトの実行が禁止されている場合でも、テキストエディターでスクリプトファイルを開くことはできます。オブジェクトの実行をブロックする場合、通知が[アプリケーション設定で有効になっている](#)と、Kaspersky Endpoint Security は標準の通知を表示します。

コンピュータネットワークの分離

[すべて表示](#) | [すべて隠す](#)

コンピュータネットワークの分離により、セキュリティ侵害インジケータ（IOC）の検知に応じてコンピュータをネットワークから自動的に分離できます。これが自動モードです。検知された脅威を調査している間に、ネットワーク分離を手動でオンにすることができます。これが手動モードです。

ネットワーク分離がオンになっている場合、アプリケーションはすべてのアクティブな接続を切断し、次の接続を除くコンピュータ上のすべての新しい TCP/IP ネットワーク接続をブロックします：

- ネットワーク分離の除外リストにリストされている接続。
- Kaspersky Endpoint Security サービスによって開始された接続。
- Kaspersky Security Center ネットワーク エージェントによって開始された接続。

重要：コンポーネント設定は Web コンソールでのみ設定できます。

自動ネットワーク分離モード

IOC 検知に応じてネットワーク分離を自動的にオンにするように設定できます。グループポリシーを使用して自動ネットワーク分離モードを設定できます。

[IOC 検知に応じてネットワーク分離を自動的にオンにするように設定する方法](#)

1. Web コンソールのメインウィンドウで、**[デバイス]** → **[タスク]** の順に選択します。
2. タスクのリストが開きます。
3. Kaspersky Endpoint Security の **IOC スキャン** をクリックします。
タスクのプロパティウィンドウが表示されます。
必要に応じて、[IOC スキャン](#) タスクを作成します。
4. **[アプリケーション設定]** タブを選択します。
5. **[IOC 検知時の処理]** ブロックで、**[IOC が見つかった後に警告し、応答処理を実行する]** をオンにし、次に **[コンピュータをネットワークから分離する (8 時間)]** をオンにします。
6. 変更を保存します。
7. これにより、IOC が検知されると、コンピュータがネットワークから分離され、脅威の拡散を防ぎます。

指定した時間が経過するとネットワーク分離が自動的にオフになるように設定できます。既定では、オンにしてから 8 時間経過するとネットワーク分離がオフになります。ネットワーク分離を手動でオフにすることもできます（次の手順を参照）：ネットワーク分離をオフにすると、コンピュータは制限なくネットワークを使用できるようになります。

[自動モードでコンピュータのネットワーク分離をオフにするための遅延を設定する方法](#)

1. Web コンソールのメインウィンドウで、**[デバイス]** → **[ポリシーとプロファイル]** の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[Detection and Response]** → **[Endpoint Detection and Response]** の順に選択します。
5. **[ネットワーク分離]** ブロックで、**[コンピュータのロック解除を設定する]** をクリックします。

6. 表示されるウィンドウで、**「分離されたコンピュータのロックを自動的に解除するまでの時間」** をオンにし、ネットワーク分離を自動的にオフにするまでの遅延時間を入力します。

7. 変更を保存します。

手動ネットワーク分離モード

ネットワーク分離を手動でオンまたはオフにすることができます。Kaspersky Security Center コンソールのコンピュータのプロパティを使用して、手動のネットワーク分離モードを設定できます。

ネットワーク分離をオンにすることができます：

- アラートの詳細（EDR Optimum のみ）：

アラートの詳細は、検知された脅威に関する収集された情報全体を表示するためのツールです。アラートの詳細には、たとえば、コンピュータに表示されるファイルの履歴が含まれます。アラートの詳細を管理する方法の詳細は、[Kaspersky Endpoint Detection and Response Optimum のヘルプ](#) を参照してください。

- ローカルアプリケーション設定を使用します。

コンピュータのネットワーク分離を手動でオンにする方法

- Web コンソールのメインウィンドウで、**「デバイス」** → **「管理対象デバイス」** の順に選択します。
- ローカルアプリケーション設定を指定するコンピュータを選択します。
これにより、コンピュータのプロパティが開きます。
- 「アプリケーション」** タブを選択します。
- 「Kaspersky Endpoint Security for Mac」** をクリックします。
これにより、ローカルアプリケーション設定が開きます。
- 「アプリケーション設定」** タブを選択します。
- 「Detection and Response」** → **「Endpoint Detection and Response」** の順に選択します。
- 「ネットワーク分離」** ブロックで、**「コンピュータをネットワークから分離する」** をクリックします。

指定した時間が経過するとネットワーク分離が自動的にオフになるように設定できます。既定では、オンにしてから 8 時間経過するとネットワーク分離がオフになります。ネットワーク分離をオフにすると、コンピュータは制限なくネットワークを使用できるようになります。

手動モードでコンピュータのネットワーク分離をオフにするための遅延を設定する方法

- Web コンソールのメインウィンドウで、**「デバイス」** → **「管理対象デバイス」** の順に選択します。
- ローカルアプリケーション設定を指定するコンピュータを選択します。
これにより、コンピュータのプロパティが開きます。
- 「タスク」** タブを選択します。
コンピュータで使用可能なタスクのリストが表示されます。
- ネットワーク分離タスク** を選択します。
- 「アプリケーション設定」** タブを選択します。
- 開いたウィンドウで、ネットワーク分離をオフにするまでの遅延を選択します。
- 変更を保存します。

コンピュータのネットワーク分離を手動でオフにする方法

- Web コンソールのメインウィンドウで、**「デバイス」** → **「管理対象デバイス」** の順に選択します。
- ローカルアプリケーション設定を指定するコンピュータを選択します。

3. これにより、コンピュータのプロパティが開きます。
4. **〔アプリケーション〕** タブを選択します。
5. **〔Kaspersky Endpoint Security for Mac〕** をクリックします。
6. これにより、ローカルアプリケーション設定が開きます。
7. **〔アプリケーション設定〕** タブを選択します。
8. **〔Detection and Response〕** → **〔Endpoint Detection and Response〕** の順に選択します。
9. **ネットワーク分離**ブロックで、**〔コンピュータの分離を解除する〕** をクリックします。

[コマンドライン](#)を使用して、ネットワーク分離をローカルで無効にすることもできます。

ネットワーク分離の除外リスト

ネットワーク分離の除外を設定できます。ネットワーク分離がオンになっている場合、ルールに一致するネットワーク接続はコンピュータ上でブロックされません。

ネットワーク分離の除外を設定するには、標準ネットワークプロファイルのリストを使用できます。既定では、除外リストには、DNS/DHCP サーバーおよび DNS/DHCP クライアントの役割を持つデバイスの中断のない動作を保証するルールを含むネットワークプロファイルが含まれます。標準ネットワークプロファイルの設定を変更したり、除外を手動で定義したりすることもできます（次の手順を参照）。

重要：ポリシーのプロパティで指定された除外は、検知された脅威に応じてネットワーク分離が自動的にオンになっている場合にのみ適用されます。コンピュータのプロパティで指定された除外は、**Kaspersky Security Center** コンソールのコンピュータのプロパティでネットワーク分離が手動でオンになっている場合にのみ適用されます。

注意：これらのパラメータには各種の使用シナリオがあるため、アクティブなポリシーでは、コンピュータのプロパティで設定されたネットワーク分離からの除外の適用を妨げることはありません。

自動モードでネットワーク分離の除外を追加する方法

1. Web コンソールのメインウィンドウで、**〔デバイス〕** → **〔ポリシーとプロファイル〕** の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
3. ポリシーのプロパティウィンドウが表示されます。
4. **〔アプリケーション設定〕** タブを選択します。
5. **〔Detection and Response〕** → **〔Endpoint Detection and Response〕** の順に選択します。
6. **〔ネットワーク分離の除外〕** ブロックで、**〔除外リスト〕** をクリックします。
7. これにより、ウィンドウが開きます。このウィンドウで、**〔プロファイルから追加〕** をクリックし、除外を設定するための標準ネットワークプロファイルを選択します。
8. プロファイルからのネットワーク分離の除外が、ネットワーク分離の除外リストに追加されます。ネットワーク接続のプロパティを表示できます。必要に応じて、ネットワーク接続設定を変更できます。
9. 必要に応じて、ネットワーク分離の除外を手動で追加します。これを行うには、除外リストのウィンドウで **〔追加〕** をクリックし、ネットワーク接続設定を手動で編集します。
10. 変更を保存します。

手動モードでネットワーク分離の除外を追加する方法

1. Web コンソールのメインウィンドウで、**〔デバイス〕** → **〔管理対象デバイス〕** の順に選択します。
2. ローカルアプリケーション設定を指定するコンピュータを選択します。
3. これにより、コンピュータのプロパティが開きます。

4. **〔タスク〕** タブを選択します。
5. コンピュータで使用可能なタスクのリストが表示されます。
6. **ネットワーク分離** タスクを選択します。
7. **〔アプリケーション設定〕** タブを選択します。
8. 表示されるウィンドウで、**〔除外リスト〕** をクリックします。
9. 次のウィンドウで、 **〔プロファイルから追加〕** をクリックし、除外を設定するための標準ネットワークプロファイルを選択します。
10. プロファイルからのネットワーク分離の除外が、ネットワーク分離の除外リストに追加されます。ネットワーク接続のプロパティを表示できます。必要に応じて、ネットワーク接続設定を変更できます。
11. 必要に応じて、ネットワーク分離の除外を手動で追加します。これを行うには、除外リストのウィンドウで **〔追加〕** をクリックし、ネットワーク接続設定を手動で編集します。
12. 変更を保存します。

[コマンドライン](#)を使用して、ネットワーク分離の除外リストをローカルで表示することもできます。この場合、コンピュータを分離する必要があります。

Cloud Sandbox

Cloud Sandbox は、コンピュータ上の高度な脅威を検知する技術です。*Kaspersky Endpoint Security* は、検知されたファイルを分析のために *Cloud Sandbox* に自動的に転送します。*Cloud Sandbox* はこれらのファイルを隔離された環境で実行し、悪意のある活動を識別してその評価を決定します。これらのファイルのデータは、*Kaspersky Security Network* に送信されます。したがって、*Cloud Sandbox* が悪意のあるファイルを検知した場合、*Kaspersky Endpoint Security* はこのファイルが検知されたすべてのコンピュータでこの脅威を排除するための適切な動作を実行します。

重要： *Cloud Sandbox* を動作させるには、[Kaspersky Security Network の使用を有効にする](#)必要があります。

注意： [Kaspersky Private Security Network](#)  を使用している場合、*Cloud Sandbox* 技術は使用できません。

Cloud Sandbox を有効にするには：

1. Web コンソールのメインウィンドウで、**〔デバイス〕** → **〔ポリシーとプロファイル〕** の順に選択します。
2. *Kaspersky Endpoint Security for Mac* ポリシーの名前をクリックします。
ポリシーのプロパティウィンドウが表示されます。
3. **〔アプリケーション設定〕** タブを選択します。
4. **〔Detection and Response〕** → **〔Endpoint Detection and Response〕** の順に選択します。
5. **〔Cloud Sandbox〕** スイッチをオンにします。
6. 変更を保存します。

脅威が存在する場合は常に、[メインウィンドウ](#)の**〔脅威の検知〕**セクションで、*Cloud Sandbox* を使用して検知された脅威のカウンターがアクティブになります。*Kaspersky Endpoint Security* は、*Kaspersky Security Center* コンソールの脅威レポートにも *Cloud Sandbox* 脅威検知技術を表示します。

FileVault ディスク暗号化

注意： *FileVault* ディスク暗号化機能は、*Kaspersky Security Center 10 SP3* 以降で使用できます。詳しくは、カスペルスキーのテクニカルサポートにお問い合わせください。

Kaspersky Endpoint Security により、*FileVault* ディスク暗号化のリモート管理が可能です。暗号化により、ユーザのコンピュータの起動ディスクに保存された機密データに対する不正なユーザアクセスを防止できます。

管理者が *Kaspersky Security Center* からコンピュータの *FileVault* 暗号化を開始すると、*Kaspersky Endpoint Security* はコンピュータのユーザに認証情報の入力进行を要求します。ディスク暗号化は、ユーザが資格情報を送信し、コンピュータが再起動され、コンピュータでポリシー設定が受信されてから **30 分** が経過した後にはのみ開始されます。資格情報の入力に要求する最小間隔も **30 分** です。

FileVault 暗号化が有効になっている時にユーザーが Mac の起動ディスクを復号化できないようにするには、管理者は JAMF を使用してディスクの復号化を禁止する MDM プロファイルを展開する必要があります。ディスクの復号化を禁止する MDM プロファイルを使用して Mac の起動ディスクを復号化するには、管理者はまずプロファイルを削除する必要があります。

注意：Kaspersky Security Center で FileVault 暗号化の管理が有効になっていない場合、管理者権限を持つユーザは、システム設定で Mac の起動ディスクを暗号化または復号化できます。FileVault の詳細は、Apple のガイドを参照してください。

コンピュータに複数のコンピュータアカウントがある場合、FileVault 暗号化を有効にすると、認証情報を入力したユーザ以外のすべてのユーザがディスクにアクセスできなくなります。

[別のユーザにディスクのロック解除を許可する ⑦](#)

1. [Apple メニュー] → [システム設定] → [プライバシーとセキュリティ] の順に選択します。
2. [FileVault] をクリックします。
[FileVault] ウィンドウが表示されます。
3. [ユーザを有効にする] をクリックします。
4. 開いたウィンドウで、コンピュータのロックを解除する権限を与えるユーザーを選択します。
5. ユーザーのコンピュータアカウントのパスワードを入力し、[OK] をクリックします。
6. [続行] をクリックします。

このユーザが暗号化されたディスクにアクセスできるようになります。

注意：別のユーザにディスクのロック解除を許可するには管理者権限が必要です。

Kaspersky Security Center 管理コンソール、Web コンソール、または Cloud コンソールを使用して Kaspersky Endpoint Security を管理すると、このコンピュータのユーザが認証情報を忘れたり紛失したりして暗号化されたディスクにアクセスできない場合、管理者は回復キーを取得できます。

[Kaspersky Security Center 管理コンソールを使用して回復キーを取得する方法](#)

[Kaspersky Security Center Web コンソールまたは Cloud コンソールを使用して回復キーを取得する方法](#)

パスワードによる保護

Kaspersky Endpoint Security では、管理者パスワードを設定することで、ユーザーデバイス上での不要な操作を制限できます。

パスワード保護が有効になっている場合、Kaspersky Endpoint Security では、次のいずれかを実行しようとする時にパスワードが要求されます：

- アプリケーション設定の変更
- 本製品の終了
- ライセンスの削除
- 本製品のアンインストール

注意：パスワード保護は、アンインストーラ経由で実行した場合にのみ、Kaspersky Endpoint Security の削除を制限します。

- バックアップからの隔離済みファイルの復元
- レポートの表示。

パスワード保護を無効にしても、ポリシー設定は無効になりません。ポリシーで設定の編集が禁止されている場合、パスワード保護が無効になっていても編集することはできません。

[管理コンソールを使用してパスワード保護を有効にする ⑧](#)

1. 管理コンソールを起動します。

2. [管理サーバー-<サーバ名>] フォルダを展開します。
3. コンソールツリーで、[管理対象デバイス] をクリックします。
4. 作業領域で、[ポリシー] タブを選択します。
5. 設定するポリシーを右クリックして [プロパティ] を選択します。
6. [プロパティ] ウィンドウで、[詳細設定] → [ユーザインターフェイス] の順に選択します。
7. [パスワードによる保護] セクションで、 [パスワードによる保護を有効にする] をオンにします。
8. 表示される [パスワードによる保護の設定] ウィンドウで、次の設定を指定します：
 - [パスワード] フィールドにパスワードを入力し、 [パスワードの確認] フィールドにもう一度入力します。
 - [パスワードが必要な操作] セクションで、ユーザのデバイス上の対応する操作を保護するために必要なチェックボックスをオンにします。
9. [OK] をクリックして変更を保存します。
10. 次のいずれかを選択し、ポリシーに変更を適用します：
 - [適用] をクリックし、 **ポリシーのプロパティ** ウィンドウが開いたままの状態に変更を保存します。
 - [OK] をクリックし、変更を保存して **ポリシーのプロパティ** ウィンドウを閉じます。

管理コンソールを使用してパスワード保護設定を編集する ②

1. 管理コンソールを起動します。
2. [管理サーバー-<サーバ名>] フォルダを展開します。
3. コンソールツリーで、[管理対象デバイス] をクリックします。
4. 作業領域で、[ポリシー] タブを選択します。
5. 設定するポリシーを右クリックして [プロパティ] を選択します。
6. [プロパティ] ウィンドウで、[詳細設定] → [ユーザインターフェイス] の順に選択します。
7. [パスワードによる保護] セクションで、 [設定] をクリックします。
8. 表示される [パスワードによる保護の設定] ウィンドウで、変更する設定を編集します。
9. [OK] をクリックして変更を保存します。

Web コンソールを使用してパスワード保護を有効にする ②

1. Web コンソールのメインウィンドウで、[デバイス] → [ポリシーとプロファイル] の順に選択します。
2. Kaspersky Endpoint Security for Mac ポリシーの名前をクリックします。
3. ポリシーのプロパティウィンドウが表示されます。
4. [アプリケーション設定] タブを選択します。
5. [詳細設定] → [ユーザインタラクション] の順に選択します。
6. [パスワードによる保護] スイッチをオンにします。
7. 表示される [パスワードによる保護の設定] ウィンドウで、次の設定を指定します：
 - [パスワード] フィールドにパスワードを入力し、 [パスワードの確認] フィールドにもう一度入力します。既定では、パスワードの文字はセキュリティ上の理由で非表示になっています。パスワードを表示するには、[表示] をクリックします。
 - [パスワードが必要な操作] セクションで、ユーザのデバイス上の対応する操作を保護するために必要なチェックボックスをオンにします。

8. [OK] をクリックして、[パスワードによる保護の設定] ダイアログを閉じます。
9. [OK] をクリックして、[ユーザインターフェイス] セクションを閉じます。
10. ポリシーへの変更を保存するには、[保存] をクリックします。

[Web コンソールを使用してパスワード保護を編集する ⑦](#)

1. Web コンソールのメインウィンドウで、[デバイス] → [ポリシーとプロファイル] の順に選択します。
2. Kaspersky Endpoint Security for Mac ポリシーの名前をクリックします。
3. ポリシーのプロパティウィンドウが表示されます。
4. [アプリケーション設定] タブを選択します。
5. [詳細設定] → [ユーザインタラクション] の順に選択します。
6. [パスワードによる保護] セクションで、[設定] をクリックします。
7. 表示される [パスワードによる保護の設定] ダイアログで、変更する設定を編集します。
8. [OK] をクリックして、[パスワードによる保護の設定] ダイアログを閉じます。
9. [OK] をクリックして、[ユーザインターフェイス] セクションを閉じます。
10. ポリシーへの変更を保存するには、[保存] をクリックします。

[Kaspersky Endpoint Security を使用してパスワード保護を有効にする ⑧](#)

1. メニューバーで製品アイコンをクリックし、[設定] を選択します。
本製品の設定ウィンドウが表示されます。
2. [インターフェイス] タブの [パスワードによる保護] セクションで、[パスワードによる保護を有効にする] をオンにします。
3. 表示されるウィンドウで、次の設定を指定します：
 - [パスワード] フィールドにパスワードを入力し、[パスワードの確認] フィールドにもう一度入力します。
 - [パスワードが必要な操作] セクションで、ユーザのデバイス上の対応する操作を保護するために必要なチェックボックスをオンにします。
4. [OK] をクリックします。

注意：パスワードにより保護される操作として [製品設定の変更] を選択すると、パスワードによる保護設定を変更するにはパスワードを 2 回入力する必要があります。

[Kaspersky Endpoint Security を使用してパスワードによる保護を編集する ⑨](#)

1. メニューバーで製品アイコンをクリックし、[設定] を選択します。
本製品の設定ウィンドウが表示されます。
2. [インターフェイス] タブの [パスワードによる保護] セクションで、[設定] をクリックします。
3. 開いたウィンドウで、変更したい設定を編集します。
4. [OK] をクリックします。

脆弱性攻撃ブロック

脆弱性攻撃ブロックは、コンピュータ上の脆弱性を悪用して管理者権限を取得したり悪意のある活動を実行しようとするプログラムコードを検知します。たとえば、脆弱性攻撃でバッファオーバーフロー攻撃が利用される可能性があります。攻撃のため、脆弱性攻撃は脆弱なアプリケーションに大量のデータを送信します。このデータを処理する際に、脆弱なアプリケーションは悪意のあるコードを実行します。この攻撃の結果、脆弱性攻撃によってマルウェアの不正インストールが開始される可能性があります。ユーザーが実行していない脆弱なアプリケーションから実行ファイルを実行しようすると、Kaspersky Endpoint Securityはこのファイルの実行をブロックするか、ユーザーに通知します。

既定では、脆弱性攻撃ブロックは有効になっています。必要に応じて、脆弱性攻撃ブロックを無効にすることができます。

[Web コンソールを使用して脆弱性攻撃ブロックを有効または無効にする](#)

1. Web コンソールのメインウィンドウで、**[アセット (デバイス)]** → **[ポリシーとプロファイル]** の順に選択します。
2. Kaspersky Endpoint Security ポリシーの名前をクリックします。
ポリシーのプロパティウィンドウが表示されます。
3. **[アプリケーション設定]** タブを選択します。
4. **[先進の脅威対策]** → **[脆弱性攻撃ブロック]** の順に選択します。
5. **[脆弱性攻撃ブロック]** スイッチをオンまたはオフにします。
6. 脆弱性攻撃ブロックをオンにする場合、脆弱性攻撃の検知時に実行する処理を次から洗濯します：

- **[ブロック](#)**

このオプションを選択すると、脆弱性攻撃の検知時に、その脆弱性攻撃による操作がブロックされて、その脆弱性攻撃に関する情報を含むログエントリが作成されます。

- **[通知する](#)**

このオプションを選択すると、脆弱性攻撃の検知時に、その脆弱性攻撃に関する情報を含むエントリがログに記録されて、アクティブな脅威のリストにその脆弱性攻撃に関する情報が追加されます。

7. 変更を保存します。

[管理コンソールを使用して脆弱性攻撃ブロックを有効または無効にする](#)

1. 管理コンソールを起動します。
2. **[管理サーバ - <サーバ名>]** フォルダを展開します。
3. コンソールツリーで、**[管理対象デバイス]** をクリックします。
4. 作業領域で、**[ポリシー]** タブを選択します。
5. 設定するポリシーを右クリックして **[プロパティ]** を選択します。
6. **[プロパティ]** ウィンドウで、**[先進の脅威対策]** → **[脆弱性攻撃ブロック]** の順に選択します。
7. **[脆弱性攻撃ブロック]** をオンまたはオフにします。
8. 必要に応じて、**[脆弱性の検知時]** セクションで、Kaspersky Endpoint Security が脆弱性攻撃を検出したときに実行する処理を選択します。
9. **[OK]** をクリックして変更を保存します。
10. 次のいずれかを選択し、ポリシーに変更を適用します：
 - **[適用]** をクリックし、**ポリシーのプロパティ** ウィンドウが開いたままの状態に変更を保存します。
 - **[OK]** をクリックし、変更を保存して**ポリシーのプロパティ** ウィンドウを閉じます。

[Kaspersky Endpoint Security を使用して脆弱性攻撃ブロックを有効または無効にする](#)

1. メニューバーで製品アイコンをクリックし、**[設定]** を選択します。

本製品の設定ウィンドウが表示されます。

2. **〔詳細〕** タブの **〔脆弱性攻撃ブロック〕** セクションで、 **〔脆弱性攻撃ブロックを有効にする〕** をオンまたはオフにします。
3. **〔ふるまい検知を有効にする〕** オンにする場合は、マルウェア活動の検知時に実行する処理を次から選択します：

- **危険なマルウェアの動作を自動でブロックする**

このオプションを選択すると、脆弱性攻撃の検知時に、その脆弱性攻撃による操作がブロックされて、その脆弱性攻撃に関する情報を含むログエントリが作成されます。

- **通知する**

このオプションを選択すると、脆弱性攻撃の検知時に、その脆弱性攻撃に関する情報を含むエントリがログに記録されて、アクティブな脅威のリストにその脆弱性攻撃に関する情報が追加されます。

脆弱性攻撃ブロックのレポートの表示

1. メニューバーで **〔プロテクション〕** → **〔レポート〕** の順に選択します。
〔レポート〕 ウィンドウが表示されます。
2. **〔脆弱性攻撃ブロック〕** タブを開きます。

修復エンジン

修復エンジンを使用すると、マルウェアがオペレーティングシステム内で行った処理をロールバックできます。

マルウェアがオペレーティングシステム内で行った動作をロールバックすると、次の種別のマルウェアの動作が処理されます：

- **ファイルの動作**

Kaspersky Endpoint Security は、次の処理を実行します：

- マルウェアによって作成された実行ファイルを削除します（ネットワークドライブ以外のすべてのメディア上の実行ファイルが対象）。
- マルウェアが侵入したプログラムによって作成された実行ファイルを削除します。
- マルウェアによって変更または削除されたファイルを復元します。

- **システムの動作**

Kaspersky Endpoint Security は、次の処理を実行します：

- マルウェアによって開始されたプロセスを終了します。
- 悪意のあるアプリケーションによって侵入されたプロセスを終了します。
- マルウェアによって停止されたプロセスは再開しません。

- **ネットワークの動作**

Kaspersky Endpoint Security は、次の処理を実行します：

- マルウェアによるネットワーク動作をブロックします。

マルウェアの処理のロールバックは、ファイル脅威対策またはふるまい検知から開始するか、マルウェアのスキャン中に開始できます。

マルウェアの動作をロールバックすると、厳密に定義されたデータセットに影響を与えます。ロールバックは、オペレーティングシステムやコンピュータのデータの整合性に悪影響を与えません。

管理コンソールでの修復エンジンの有効化または無効化

1. 管理コンソールを起動します。
2. **〔管理サーバ - <サーバ名>〕** フォルダを展開します。
3. コンソールツリーで、**〔管理対象デバイス〕** をクリックします。

4. 作業領域で、[ポリシー] タブを選択します。
5. 設定するポリシーを右クリックして [プロパティ] を選択します。
6. [プロパティ] ウィンドウで、[先進の脅威対策] → [修復エンジン] の順に選択します。
7. [修復エンジン] をオンまたはオフにします。
8. [OK] をクリックして変更を保存します。
9. 次のいずれかを選択し、ポリシーに変更を適用します：
 - [適用] をクリックし、**ポリシーのプロパティ** ウィンドウが開いたままの状態に変更を保存します。
 - [OK] をクリックし、変更を保存して**ポリシーのプロパティ** ウィンドウを閉じます。

[Web コンソールでの修復エンジンの有効化または無効化](#)

1. Web コンソールのメインウィンドウで、[アセット (デバイス)] → [ポリシーとプロファイル] の順に選択します。
2. Kaspersky Endpoint Security ポリシーの名前をクリックします。
ポリシーのプロパティ ウィンドウが表示されます。
3. [アプリケーション設定] タブを選択します。
4. [先進の脅威対策] → [修復エンジン] の順に移動します。
5. [修復エンジン] スイッチをオンまたはオフにします。
6. 変更を保存します。

[製品インターフェイスでの修復エンジンの有効化または無効化](#)

1. メニューバーで製品アイコンをクリックし、[設定] を選択します。
本製品の設定ウィンドウが表示されます。
2. [詳細] タブの [修復エンジン] セクションで、[修復エンジンを有効にする] をオンまたはオフにします。

これにより、修復エンジンが有効になると、悪意のあるアプリケーションによって実行されたオペレーティングシステム内での処理がロールバックされます。

ウェブコントロール

[すべて表示](#) | [すべて隠す](#)

ウェブコントロールでは、ユーザによる Web リソースへのアクセスが管理されます。これにより、トラフィック量や就業時間の不適切な使用が削減されます。ユーザがウェブコントロールによって制限されている Web サイトを開こうとすると、Kaspersky Endpoint Security はアクセスをブロックするか、警告を表示します。

特定の Web サイトまたは選択したカテゴリの Web サイトへのアクセスをブロックできます。

注意：Kaspersky Endpoint Security がブロックできるのは、接続に HTTPS を使用している Web サイトへのアクセスのみです。[脅威対策] タブの [全般] セクションにある [セキュアな接続 (HTTPS) をチェックする] をオンにしている場合にのみ、暗号化された接続 (HTTPS) がスキャンされます。

[管理コンソールでの新しいルールの追加](#)

1. 管理コンソールを起動します。
2. [管理サーバ - <サーバ名>] フォルダを展開します。
3. コンソールツリーで、[管理対象デバイス] をクリックします。
4. 作業領域で、[ポリシー] タブを選択します。

5. 設定するポリシーを右クリックして **「プロパティ」** を選択します。
6. **「プロパティ」** ウィンドウで、**「セキュリティコントロール」** → **「ウェブコントロール」** の順に選択します。
7. **「ウェブコントロールを有効にする」** をオンにします。
8. **「追加」** をクリックします。
9. 表示されたウィンドウで、ルール名を入力します。
10. ルールをアクティブにする場合は、**「使用中のルール」** をオンにします。
11. 次のいずれかを実行します：
 - 特定の URL にルールを適用する場合は、**「URL または URL のグループ（マスク）」** をオンにします。
 - 特定の Web サイトのカテゴリにルールを適用する場合は、**「Web サイトのカテゴリ」** をオンにします。
12. **「指定」** をクリックします。
13. 表示されるウィンドウで、ルールの範囲を指定します。
14. 次のいずれかを実行します：
 - アクセスをブロックする場合は、**「ブロック」** をオンにします。
 - アクセスを許可する場合は、**「許可」** をオンにします。
 - 警告を表示する場合は、**「警告を表示」** をオンにします。
15. **「OK」** をクリックして変更を保存します。
16. 次のいずれかを選択し、ポリシーに変更を適用します：
 - **「適用」** をクリックし、**ポリシーのプロパティ** ウィンドウが開いたままの状態に変更を保存します。
 - **「OK」** をクリックし、変更を保存して **ポリシーのプロパティ** ウィンドウを閉じます。

Web コンソールでの新しいルールの追加

1. Web コンソールのメインウィンドウで、**「アセット（デバイス）」** → **「ポリシーとプロファイル」** の順に選択します。
2. Kaspersky Endpoint Security ポリシーの名前をクリックします。
ポリシーのプロパティウィンドウが表示されます。
3. **「アプリケーション設定」** タブを選択します。
4. **「セキュリティコントロール」** → **「ウェブコントロール」** の順に移動します。
5. **「ウェブコントロール」** スイッチをオンにします。
6. **「追加」** をクリックします。
7. 表示されたウィンドウで、ルール名を入力します。
8. 次のいずれかを実行します：
 - ルールをアクティブにする場合は、**「アクティブ」** をオンにします。
 - ルールを非アクティブにする場合は、**「非アクティブ」** をオンにします。
9. 次のいずれかを実行します：
 - アクセスを許可する場合は、**「許可」** をオンにします。
 - アクセスをブロックする場合は、**「ブロック」** をオンにします。
 - 警告を表示する場合は、**「警告を表示」** をオンにします。
10. 次のいずれかを実行します：

- 特定の Web サイトのカテゴリにルールを適用する場合は、[カテゴリ] をオンにして、[カテゴリを選択] をクリックしてカテゴリを選択します。
- 特定の URL にルールを適用する場合は、[個別のアドレス] をオンにして、下の表に追加します。

11. 変更を保存します。

注意：ウェブコントロール設定は、Kaspersky Endpoint Security では管理できません。

デバイスコントロール

デバイスコントロールによって、コンピュータにインストールされているデバイスまたはコンピュータに接続されているデバイスへのユーザアクセスが管理されます。これにより、こうしたデバイスの接続時にコンピュータを感染から保護し、データの損失や漏えいを防ぐことができます。

デバイスへのアクセスの判定基準

デバイスコントロールは、次の情報に基づいてアクセスを制御できます：

- **デバイス種別：**プリンター、リムーバブルドライブ、CD/DVD ドライブなどの種別。

次のようにデバイスアクセスを設定できます：

- 許可：
- ブロック：
- 例外を除きブロック（Wi-Fi のみ）。

- **信頼するデバイス：**「信頼するデバイス」は、信頼するデバイスの設定で指定されたユーザが常にフルアクセスできるデバイスです。

次のデータに基づいて信頼するデバイスを追加できます：

- **ID によるデバイス：**各デバイスには固有の識別子があります（ハードウェア ID、または HWID）。これらの ID は、オペレーティングシステムのツールを使用してデバイスのプロパティで確認できます。デバイス ID の例：
SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000。特定のデバイスを複数追加する場合は、ID でデバイスを追加すると便利です。
- **モデルによるデバイス：**各デバイスには製造元 ID（VID）および製品 ID（PID）があります。これらの ID は、オペレーティングシステムのツールを使用してデバイスのプロパティで確認できます。VID および PID の入力用テンプレート：VID_1234&PID_5678。組織内で特定のモデルのデバイスを使用する場合は、モデルでデバイスを追加すると便利です。この方法を使用することで、このモデルのデバイスをすべて追加できます。
- **ID マスクによるデバイス：**類似の ID を持つ複数のデバイスを使用している場合、マスクを使用してデバイスを信頼リストに追加できます。
* 文字は、任意の文字列を置き換えます。Kaspersky Endpoint Security では、マスクでの「?」記号の使用をサポートしていません。例：
WDC_C*。
- **モデルマスクによるデバイス：**類似の VID または PID を持つ複数のデバイス（たとえば、製作元が同じデバイス）を使用している場合、マスクを使用してデバイスを信頼リストへ追加できます。* 文字は、任意の文字列を置き換えます。Kaspersky Endpoint Security では、マスクでの「?」記号の使用をサポートしていません。例：VID_05AC&PID_*。

管理コンソールでのデバイスコントロールの管理

1. 管理コンソールを起動します。
2. [管理サーバ - <サーバ名>] フォルダを展開します。
3. コンソールツリーで、[管理対象デバイス] をクリックします。
4. 作業領域で、[ポリシー] タブを選択します。
5. 設定するポリシーを右クリックして [プロパティ] を選択します。
6. [プロパティ] ウィンドウで、[セキュリティコントロール] → [デバイスコントロール] の順に選択します。
7. [デバイスコントロール] をオンにします。
8. [デバイス種別] タブで、デバイス種別と Wi-Fi ネットワークについてのアクセスルールを設定します。
9. [信頼するデバイス] タブで、個々のデバイスまたはデバイスグループについてのアクセスルールを設定します。

10. [OK] をクリックして変更を保存します。
11. 次のいずれかを選択し、ポリシーに変更を適用します：
 - [適用] をクリックし、**ポリシーのプロパティ** ウィンドウが開いたままの状態に変更を保存します。
 - [OK] をクリックし、変更を保存して**ポリシーのプロパティ** ウィンドウを閉じます。

[Web コンソールでのデバイスコントロールの管理](#)

1. Web コンソールのメインウィンドウで、[アセット (デバイス)] → [ポリシーとプロファイル] の順に選択します。
2. Kaspersky Endpoint Security のポリシーの名前をクリックします。
ポリシーのプロパティ ウィンドウが表示されます。
3. [アプリケーション設定] タブを選択します。
4. [セキュリティコントロール] → [デバイスコントロール] の順に移動します。
5. [デバイスコントロール] スイッチをオンにします。
6. [デバイスコントロールの設定] セクションで、デバイス、デバイス種別、Wi-Fi ネットワークについてのアクセスルールを設定します。
7. 変更を保存します。

注意： デバイスコントロール設定は、Kaspersky Endpoint Security では管理できません。

そのため、デバイスコントロールが有効になると、本製品は接続されているデバイスの情報を Kaspersky Security Center に渡します。接続されたデバイスのリストは Kaspersky Security Center の [詳細] → [リポジトリ] → [ハードウェア] フォルダで表示できます。

[デバイスコントロールのレポートの表示](#)

1. メニューバーで [プロテクション] → [レポート] の順に選択します。
[レポート] ウィンドウが表示されます。
2. [デバイスコントロール] タブを開きます。

Kaspersky Security Network に参加する

[Kaspersky Security Network](#) に参加すると、Kaspersky Endpoint Security の統計が自動的にカスペルスキーに送信され、Mac をより強力に保護できるようになります。

注意： カスペルスキーでは、お客様の明確な同意がない限り、いかなる個人情報の受信、処理、保管も行いません。

Kaspersky Security Network への参加は任意です。参加するかどうかは、Kaspersky Endpoint Security のインストール時に決定します。ただし、インストール後にいつでも変更できます。

[Kaspersky Security Network を有効にする](#)

1. メニューバーで製品アイコンをクリックし、[設定] を選択します。
本製品の設定ウィンドウが表示されます。
2. [詳細] タブの [KSN] セクションで、[KSN 声明を表示する] をクリックして Kaspersky Security Network に関する声明を表示します。
3. ファイル、Web リソース、アプリケーションの評価情報を Kaspersky Security Network から受信して本製品で使用するのを希望し、声明のすべての条項に同意する場合、[Kaspersky Security Network に参加する] をオンにします。
4. 表示されるウィンドウで、[同意する] をクリックします。

[Kaspersky Security Network に参加する] と [拡張 KSN モードを有効にする] がオンになります。

注意：既定では、拡張 KSN モードが使用されます。拡張 KSN モードでは、本製品からカスペルスキーへ詳細データが送信されます。データをカスペルスキーへ提供しない場合は、**「拡張 KSN モードを有効にする」** をオフにしてください。

Kaspersky Security Network の使用時にカスペルスキーに提供されるデータ ②

「Kaspersky Security Network に参加する」 をオンにし、**「拡張 KSN モードを有効にする」** をオフにすると、次のデータがカスペルスキーに提供されます：

- 適用されているライセンスの情報：ライセンスの種別および有効期間、ライセンスの有効期限までの日数、ライセンスの購入元である代理店の識別子、地域のアクティベーションセンターの識別子、アクティベーションコードのチェックサム、SHA1 アルゴリズムを使用して計算されたチケットボディのハッシュ、ライセンスチケットの作成日時、ライセンス情報の識別子、ライセンスチケットの識別子、ライセンスチケットのシーケンスの識別子、ユーザのコンピュータの一意な識別子、ライセンスチケットが有効になった日付、ライセンスチケットの有効期限、ライセンスチケットの現在のステータス、チケットヘッダーのバージョン、ライセンスのバージョン、チケットヘッダーの署名に使用された証明書の識別子、ライセンスファイルのチェックサム、チケットヘッダーの署名元のシリアル番号、認証トークン。
- インストールされた本ソフトウェアの詳細バージョン。

インストールされた本ソフトウェアの種別。ソフトウェアアップデートの ID。評価サービスの ID。プロトコルタイプの ID。地域のアクティベーションセンターの ID。本ソフトウェアのサービスの決定のうち取り消されたもののリストのバージョン。トリガーされた本ソフトウェアの定義データベースのレコードの ID。トリガーされた本ソフトウェアの定義データベースのレコードのタイムスタンプ。トリガーされた本ソフトウェアの定義データベースのレコードの種別。本ソフトウェアのコンピュータへのインストールのインスタンスの一意な ID。ライセンスがアクティベートされた日付。ライセンスの有効期限日。ライセンスの識別子。本ソフトウェアが使用中のライセンスのステータス。処理中のオブジェクトのチェックサム種別。検知されたマルウェアの名前、ユーザのコンピュータまたはデータに損害を与える目的で使用される可能性がある正規のソフトウェアの名前。処理中のオブジェクトのチェックサム。本ソフトウェアのアクティベーションコードのチェックサム。本ソフトウェアの詳細バージョン。一意のデバイス ID。本ソフトウェアの ID。本ソフトウェアのライセンス情報ファイルのチェックサム。本ソフトウェアのライセンスの提供に使用された情報形式の ID。本ソフトウェアのライセンスチケットのヘッダーへの署名に使用される証明書の識別子。本ソフトウェアのライセンスチケットの作成日時。本ソフトウェアのライセンスチケットのチェックサム。本ソフトウェアのライセンスチケットのバージョン。本ソフトウェアのアクティベーションコードのバージョン。権利者のインフラストラクチャへのリクエストに含まれるデータの形式。使用中のライセンスチケットの ID。本ソフトウェアのコンポーネントの ID。本ソフトウェアの動作の結果。エラーコード。アクセスされた Web サービスのアドレス (URL、IP)。ポート番号。Web サービスのリクエスト元の URL (リファラー)。証明書の公開鍵。スキャンされたオブジェクトのデジタル証明書のサムプリントとハッシュアルゴリズム。

「Kaspersky Security Network に参加する」 と **「拡張 KSN モードを有効にする」** をオンにすると、次のデータがカスペルスキーに提供されます：

- コンピュータにインストールされているオペレーティングシステム (OS) やサービスパックのバージョンに関する情報、OS カーネルファイルのバージョンおよびチェックサム (MD5、SHA2-256、SHA1)、OS 実行モードの識別子。OS のバージョン、OS のビルド番号、OS のアップデート番号、OS のエディション、OS のエディションに関する詳細情報。OS のサービスパックのバージョン OS の起動日時。ふるまい分析のサブシステムにおける OS 動作に関するイベントの処理遅延時間。現在の種別の遅延された OS 動作イベントの数。プロアクティブディフェンスのサブシステムにおける OS 動作に関するイベントの処理遅延時間。処理された OS 動作イベントの数。処理された OS 同期動作イベントの数。現在の種別のすべての OS 動作イベントの合計遅延時間。持続的イベントを記憶するサブシステムにおける、OS 動作に関するイベントの処理遅延時間。すべての OS 動作イベントの合計遅延。待機中の OS 同期動作イベントの数。OS 内の動作イベントを受信した日時。
- 以前、OS の再起動が失敗した履歴：再起動に失敗した回数。
- インストールされている本製品に関する情報およびアンチウイルス保護状況：ソフトウェアのインストール識別子 (PCID) 本ソフトウェアの定義データベースのレコードのバージョン、コンピューター上にインストールされたアプリケーションのインスタンスの一意な識別子、アプリケーションの種別、アプリケーション種別の識別子、インストールされたアプリケーションの詳細バージョン、アプリケーションの設定のバージョンの識別子、コンピューター種別の識別子、アプリケーションがインストールされたコンピューターの一意な識別子、権利者のサービスにおける一意なユーザー識別子、言語および動作状況、インストールされたソフトウェアコンポーネントのバージョンと動作状況、権利者のサービスに接続するために使用されたプロトコルのバージョン、インストールされた本ソフトウェアの詳細バージョン。インストールされた本ソフトウェアの種別。ソフトウェアアップデートの ID。評価サービスの ID。プロトコルタイプの ID。地域のアクティベーションセンターの ID。本ソフトウェアのサービスの決定のうち取り消されたもののリストのバージョン。トリガーされた本ソフトウェアの定義データベースのレコードの ID。トリガーされた本ソフトウェアの定義データベースのレコードのタイムスタンプ。トリガーされた本ソフトウェアの定義データベースのレコードの種別。本ソフトウェアのコンピュータへのインストールのインスタンスの一意な ID。ライセンスがアクティベートされた日付。ライセンスの有効期限日。ライセンスの識別子。本ソフトウェアが使用中のライセンスのステータス。処理中のオブジェクトのチェックサム種別。検知されたマルウェアの名前、ユーザのコンピュータまたはデータに損害を与える目的で使用される可能性がある正規のソフトウェアの名前。処理中のオブジェクトのチェックサム。本ソフトウェアのアクティベーションコードのチェックサム。本ソフトウェアの詳細バージョン。本ソフトウェアの ID。本ソフトウェアのライセンス情報ファイルのチェックサム。本ソフトウェアのライセンスの提供に使用された情報形式の ID。本ソフトウェアのライセンスチケットのヘッダーへの署名に使用される証明書の識別子。本ソフトウェアのライセンスチケットの作成日時。本ソフトウェアのライセンスチケットのチェックサム。本ソフトウェアのライセンスチケットのバージョン。本ソフトウェアのアクティベーションコードのバージョン。権利者のインフラストラクチャへのリクエストに含まれるデータの形式。使用中のライセンスチケットの ID。本ソフトウェアのコンポーネントの ID。本ソフトウェアの動作の結果。エラーコード。アクセスされた Web サービスのアドレス (URL、IP)。ポート番号。Web サービスのリクエスト元の URL (リファラー)。定義データベースのアップデートと適用のサイクル数。定義データベースが最後にアップデートおよび適用された日時。本ソフトウェアの定義データベースの公開日時。本ソフトウェアのコンポーネントのバージョン。ソフトウェアアップデートの ID。インストールされた本ソフトウェアの種別。システムウォッチャーの開始日時。本ソフトウェアのインストール日時。システムウォッチャーによって統計が送信される確率。システムウォッチャーによる標準処理時間よりも長い時間がかかったイベントのコード。システムウォッチャーによる標準処理時間を超えたイベントのデータベース処理時間。システムウォッチャーによるイベントの処理に許可される最大時間。システムウォッチャーによる標準処理時間を超えたイベントの処理時間。システムウォッチャーによる標準処理時間よりも長い時間がかかったイベントの総数。

- 処理したすべてのオブジェクトおよび操作に関する情報：処理中のオブジェクトに対する本ソフトウェアの判定、ディレクトリコード、処理中のオブジェクトのサイズ、処理中のオブジェクトのチェックサム（SHA256）、システムウォッチャーを使用して検知されたソフトウェアの数、システムウォッチャーでソフトウェアを検知した日時、検知の特性、トリガーされた本ソフトウェアの定義データベースのレコードのID。システムウォッチャーでソフトウェアを検知した理由、処理中のオブジェクトのチェックサム（MD5）、モジュールの整合性チェックの結果、処理中のオブジェクトの名前、トリガーされた本ソフトウェアの定義データベースのレコードの種別、処理中のオブジェクトへのパス。スキャンしたオブジェクトの製造元の名前、スキャンの日時、URL およびダウンロードされたリファラーのアドレス、スキャンされたファイルのサイズおよびパス、アーカイブかどうかのフラグ、ファイルの作成日時、圧縮されていた場合はパッカーの名前、サイズおよびチェックサム（MD5、SHA2-256）、ファイルのエントロピー、ファイルの種別、ファイル種別コード、ファイルが実行可能であるかどうかのフラグ、識別子および形式、オブジェクトのチェックサム（MD5、SHA2-256）、オブジェクトの追加チェックサムの種別および値、オブジェクトのデジタル署名（証明書）に関するデータ：証明書の発行元に関する情報、前回の統計が送信されてからオブジェクトが実行された回数、本製品のスキャンタスクの識別子、オブジェクトの評価に関する情報の受信手段、TARGET フィルターの値、適用可能な検知技術の技術的パラメータ。処理中のオブジェクトへのパス。ディレクトリコード。
- 実行ファイルの場合：ファイルセクションの情報量、評価の検証フラグまたはファイルの署名フラグ、検証対象のオブジェクトに読み込まれたアプリケーションの名前、種別、ID 種別、チェックサム（MD5）およびサイズ、アプリケーションのパスおよびテンプレートのパス、自動実行リストの署名、エントリの日時、属性のリスト、圧縮ソフトウェアの名前、アプリケーションのデジタル署名に関する情報：発行者の証明書、アップロードされたファイルの MIME 形式での名前、ファイルが作成された日時。
- 実行中のアプリケーションおよびそのモジュールに関する情報：実行中のファイルのチェックサム（MD5、SHA2-256）、ファイルのサイズ、属性、作成日時、圧縮ソフトウェアの名前（ファイルが圧縮されている場合）、ファイル名、システム上で実行されているプロセスに関する情報（プロセス ID（PID）、プロセス名、プロセスを開始したアカウントに関する情報、プロセスを開始したアプリケーションおよびコマンド、プロセスのファイルへの完全パスおよび開始したコマンドライン、プロセスが属するアプリケーションの説明（アプリケーション名および配信元の情報）、使用されるデジタル証明書およびそれらの正当性を検証するために必要な情報またはファイルのデジタル署名が存在しない旨のフラグ）、プロセスに読み込まれたモジュールの情報：名前、サイズ、種別、作成日、属性、チェックサム（MD5、SHA2-256、SHA1）およびパス、PE ファイルのヘッダー情報、圧縮ソフトウェア名（ファイルが圧縮されている場合）、統計情報の有効性および使用可否に関する情報、送信される統計情報の生成条件の識別子。
- 脅威または脆弱性が検知された場合、検知されたオブジェクトに関する情報に加え、次の情報が提供されます：定義データベース中のレコードの識別子、バージョンおよび種別、カスペルスキーの分類による脅威名、定義データベースの最終アップデート日時、実行ファイルの名前、脅威が検知された URL をリクエストしたアプリケーションのファイルのチェックサム（MD5）、検知した脅威の IP アドレス（IPv4 または IPv6）、脆弱性の識別子および脅威レベル、脅威を検知した Web ページの URL およびリファラー。
- 悪意のある可能性があるオブジェクトが検知された場合、プロセスのメモリ内のデータに関する情報が提供されます。
- ネットワーク攻撃の情報：攻撃元コンピュータの IP アドレスおよびユーザのコンピュータ上でネットワーク攻撃の標的にされたポート番号、攻撃プロトコルの ID、名前および攻撃種別。
- ネットワーク接続に関する情報：ポートを開いたプロセスを起動したファイルのバージョンおよびチェックサム（MD5、SHA2-256、SHA1）、プロセスのファイルのパスおよびデジタル署名、ローカルおよびリモートの IP アドレス、ローカルおよびリモート接続のポート番号、接続状況、ポートが開かれた時刻。
- 危険なオブジェクトまたは疑わしいオブジェクトを検知した Web ページの URL および IP アドレス、この URL をリクエストしたファイルの名前、サイズおよびチェックサム、識別子、検知結果の決定基準に使用されたルールの重み係数および度数、攻撃の目的に関する情報。
- インストール済み本ソフトウェアおよび定義データベースのアップデートに関する情報：アップデートタスクの完了状況、アップデート中に発生した可能性のあるエラーの種別、失敗したアップデートの数、アップデートを実行した本ソフトウェア機能の識別子。
- Kaspersky Security Network（KSN）の使用に関する情報：KSN の識別子、本ソフトウェアの識別子、本ソフトウェアの詳細バージョン、個人を特定できないようにしたお客様のデバイスの IP アドレス、KSN へのリクエストの実行品質を示す指数、KSN 用パケットの処理品質を示す指数、KSN へのリクエストの件数およびリクエストの種別に関する情報、統計情報の送信を開始した日時と終了した日時、KSN 設定のアップデートに関する情報：アクティブな設定の識別子、受信した設定の識別子、設定のアップデートのエラーコード。
- イベントに関するシステムログ内の情報：イベントのタイムスタンプ、イベントが検知されたログの名前、イベントの種別およびカテゴリ、イベントの発生源の名前およびイベントの説明。
- ファイルおよび URL の評価決定に関する情報：評価が要求された URL とその参照元、接続のプロトコルタイプ、アプリケーション種別の内部識別子、使用されているポートの番号、ユーザ識別子、スキャンされたファイルのチェックサム（MD5）、検知された脅威の種別、脅威の検知に使用したレコードに関する情報（定義データベースのレコードの識別子、レコードのタイムスタンプと種別）。証明書の公開鍵。スキャンされたオブジェクトのデジタル証明書のサムプリントとハッシュアルゴリズム。
- 本ソフトウェアの地域分布に関する情報：本ソフトウェアのインストールおよびアクティベーションの日時、本ソフトウェアのアクティベーション用のライセンスを提供した代理店の識別子、本ソフトウェアの識別子、本ソフトウェアの言語版の識別子、本ソフトウェアに適用されたライセンスの識別番号、KSN に参加しているかどうかのフラグ。
- 適用されているライセンスの情報：ライセンスの種別および有効期間、ライセンスの有効期限までの日数、ライセンスの購入元である代理店の識別子、地域のアクティベーションセンターの識別子、アクティベーションコードのチェックサム、SHA1 アルゴリズムを使用して計算されたチケットボディのハッシュ、ライセンスチケットの作成日時、ライセンス情報の識別子、ライセンスチケットの識別子、ライセンスチケットのシーケンスの識別子、ユーザのコンピュータの一意な識別子、ライセンスチケットが有効になった日付、ライセンスチケットの有効期限、ライセンスチケットの現在のステータス、チケットヘッダーのバージョン、ライセンスのバージョン、チケットヘッダーの署名に使用された証明書の識別子、ライセンスファイルのチェックサム、チケットヘッダーの署名元のシリアル番号、認証トークン。
- コンピュータにインストールされているハードウェアに関する情報：搭載または接続された装置の種別、名前、機種名、ファームウェアのバージョン、パラメータ。

- 端末に関する情報： 端末の識別子。

- ウェブコントロール機能の動作に関する情報：

機能のバージョン、当該カテゴリに分類された理由および関連情報、分類された URL、ブロックまたは分類されたオブジェクトのホストの IP アドレス。

注意：Kaspersky Security Center の設定に応じて、Kaspersky Security Network の代わりに Kaspersky Private Security Network への参加を行うことができます。Kaspersky Endpoint Security は、Kaspersky Private Security Network から Kaspersky Security Network に切り替えることを通知し、Kaspersky Security Network に関する声明の条件に同意するよう要求します。Kaspersky Private Security Network への参加に関する詳細は、[Kaspersky Security Center のヘルプ](#) を参照してください。

Kaspersky Security Network インフラストラクチャ

Kaspersky Endpoint Security がサポートする Kaspersky Security Network インフラストラクチャのソリューションは次の通りです：

- グローバル KSN は、ほとんどのカスペルスキー製品で使用されています。KSN の参加者は、Kaspersky Security Network から情報を受信します。また、ユーザのコンピュータで検知されたオブジェクトに関する情報をカスペルスキーに送信します。送信された情報をカスペルスキーのアナリストがさらに分析し、Kaspersky Security Network の統計情報データベースにその評価を追加します。
- プライベート KSN を使用すると、Kaspersky Endpoint Security やその他のカスペルスキー製品を使用するコンピュータのユーザが、Kaspersky Security Network の評価データベースやその他の統計情報にアクセスできるようになります。コンピュータから Kaspersky Security Network へデータは送信されません。プライベート KSN は、次のいずれかの理由により Kaspersky Security Network へ参加できない企業ユーザのお客様のために設計されています：
 - ローカルワークステーションがインターネットに接続されていない。
 - 国外、または企業内 LAN の外部へのデータ送信が、法律または企業のセキュリティポリシーにより禁止されている。

既定では、Kaspersky Security Center はグローバル KSN を使用します。プライベート KSN の使用は、Kaspersky Security Center 管理コンソール (MMC) と Kaspersky Security Center Web コンソールで設定できます。プライベート KSN は、Kaspersky Security Center Cloud コンソールでは使用できません。

KSN プロキシ

Kaspersky Security Center 管理サーバーが管理するコンピュータは、KSN プロキシサービスを使用して Kaspersky Security Network と対話できます。

KSN プロキシサービスにより可能な動作は次の通りです：

- ユーザのコンピュータが、インターネットへ直接アクセスすることなく、クエリや情報を KSN へ送信できます。
- KSN プロキシサービスが処理済みデータをキャッシュするので、外部ネットワークへの通信チャネルの負荷が軽減され、ユーザのコンピュータが要求した情報の受信する速度が向上します。

KSN プロキシサービスの詳細は、[Kaspersky Security Center のヘルプ](#) を参照してください。

ご注意：アップデート機能（マルウェア対策の署名のアップデートおよびコードベースのアップデートの提供を含む）および KSN 機能は、アメリカ合衆国内にある本ソフトウェアではご利用いただけなくなる可能性があります。

製品コンポーネントの整合性をチェックする

Kaspersky Endpoint Security には、ダイナミックリンクライブラリ、実行ファイル、設定情報ファイル、インターフェイスファイルの形式で、様々なバイナリモジュールが含まれています。侵入者により、1つ以上のアプリケーションの実行モジュールまたはファイルが、悪意のあるコードを含む別のファイルに置換される場合があります。これを防止するために、Kaspersky Endpoint Security は製品コンポーネントの整合性をチェックすることができます。本製品は、モジュールとファイルが、許諾なく変更されたり破損されたりしていないかどうかチェックします。製品モジュールまたはファイルのチェックサムが正しくない場合、破損が発生したと判断されます。

ディレクトリ `/Library/Application Support/Kaspersky Lab/KAV/Binaries` にある `integrity_checker` ユーティリティを使用して、製品コンポーネントの整合性がチェックされます。このユーティリティは、製品コンポーネントの正常な動作にとってその整合性が重大であるアプリケーションファイルのリストが含まれるマニフェストファイルの整合性をチェックします。

カスペルスキーの暗号署名で保護されたマニフェストファイル `integrity_check.xml` は、`integrity_checker utility` と同じディレクトリに配置されています (`/Library/Application Support/Kaspersky Lab/KAV/Binaries`)。

注意： ルートユーザアカウントの権限が、`integrity_checker utility` の実行に必要です。

整合性チェックは、本製品と一緒にインストールされたユーティリティ、または認定済み CD に同梱されたユーティリティを使用して実行できます。

製品コンポーネントの整合性をチェックするには、次のコマンドを実行します：

```
sudo "/Library/Application Support/Kaspersky Lab/KAV/Binaries/integrity_checker"
```

既定では、ユーティリティはディレクトリ `/Library/Application Support/Kaspersky Lab/KAV/Binaries` にあるファイル `integrity_check.xml` を使用します。

ユーティリティ設定のヘルプを表示するには、次のコマンドを実行します：

```
--help
```

各マニフェストファイルのチェック結果は、マニフェストファイルの名前の隣に、次の形式で表示されます：

- **SUCCEEDED**—ファイルの整合性が確認されました（リターンコード：0）
- **FAILED**—ファイルの整合性が確認されませんでした（リターンコード：0 以外）

Kaspersky Security Center 管理コンソールからの製品の管理

Kaspersky Security Center は、企業のネットワークのセキュリティの一元管理を目的としています。Kaspersky Security Centerの詳細は、[Kaspersky Security Center のヘルプ](#) を参照してください。

Kaspersky Endpoint Security を、[製品のグラフィカルユーザインターフェイス](#)、[Kaspersky Security Center Web コンソール](#)または [Cloud コンソール](#)、または[コマンドライン](#)から管理することもできます。

企業ネットワークに Kaspersky Endpoint Security を導入する

1. （ネットワークに管理サーバーを導入します。

管理サーバーとは、Kaspersky Security Center のコンポーネントで、企業ネットワークにインストールされているすべてのカスペルスキー製品に関する情報を一元的に保管し、これらの製品を管理します。

2. Kaspersky Security Center の管理者用ワークステーションに管理コンソールをインストールします。

管理コンソールとは、Kaspersky Security Center のコンポーネントで、管理サーバーとネットワークエージェントの管理サービス用にユーザインターフェイスを提供します。ネットワークエージェントは、管理サーバーと企業ネットワークのコンピュータにインストールされている Kaspersky Endpoint Security との対話を調整します。

3. [Kaspersky Security Center](#) の管理者用ワークステーションに、[Kaspersky Endpoint Security](#) の管理プラグインをインストールします。

管理プラグインは、管理コンソールからカスペルスキー製品を管理するためのインターフェイスを提供する専用コンポーネントです。製品ごとに独自の管理プラグインがあります。管理プラグインは、Kaspersky Security Center を使用して管理できるすべてのカスペルスキー製品に提供されています。

4. 次のいずれかの方法で、リモートの Mac コンピュータにネットワークエージェントをインストールします：

- [ローカルで](#)
- [Apple Remote Desktop を使用してリモートで](#)
- [Kaspersky Security Center を使用してリモートで](#)
- [SSH プロトコルを使用してリモートで](#)

注意： Kaspersky Security Center を使用して Kaspersky Endpoint Security for Mac 12.2 を管理するには、ネットワークエージェントのバージョン 15 をリモートコンピュータにインストールする必要があります。

5. 次のいずれかの方法で、リモートの Mac コンピュータに Kaspersky Endpoint Security をインストールします：

- [ローカルで](#)
- [Apple Remote Desktop を使用してリモートで](#)
- [SSH プロトコルを使用してリモートで](#)
- [Kaspersky Security Center を使用してリモートで](#)

重要：カスペルスキー インターネット セキュリティ for Mac またはサードパーティ製のマルウェア対策製品がリモートのコンピュータにインストールされている場合は、Kaspersky Endpoint Security のインストール前にこれらの製品をアンインストールしてください。

管理サーバーの導入および管理コンソールのインストール方法の詳細は、[Kaspersky Security Center のヘルプ](#) を参照してください。

Kaspersky Endpoint Security バージョン 11.1 以降をバージョン 12.2 にアップデート

注意：Kaspersky Security Center を使用して Kaspersky Endpoint Security for Mac 12.2 を管理するには、ネットワークエージェントのバージョン 15 をリモートコンピュータにインストールする必要があります。

次のいずれかの方法で、Kaspersky Security Center 経由で管理されている Kaspersky Endpoint Security をバージョン 11.1 以降からバージョン 12.2 にアップデートできます：

- リモートコンピュータ上で、Kaspersky Endpoint Security をバージョン 12.2 に、ネットワークエージェントをバージョン 15 に同時にアップデートします。
- ネットワークエージェントをバージョン 15 にアップデートしてから Kaspersky Endpoint Security をバージョン 12.2 にアップデートします。

本製品を新バージョンへアップデートする際、次を考慮してください：

- Kaspersky Endpoint Security をバージョン 12.2 にアップデートするには、macOS 12 以降が必要です。
- [テクニカルサポートサイト](#) からアーカイブ KES_11.3_profile.zip をダウンロードして、新しい構成プロファイルを適用する必要があります。
- Kaspersky Endpoint Security をバージョン 12.2 へアップデートした後、Kaspersky Filter と 2 つの Kaspersky Monitor がネットワーク設定に表示される場合があります。
- Kaspersky Endpoint Security バージョン 11.0.1 以前を使用している場合、バージョン 12.2 にアップデートするには、本製品をアンインストールし、macOS をバージョン 12 以降にアップデートする必要があります。その後、Kaspersky Endpoint Security バージョン 12.2 のインストールが可能になります。

ご注意：アップデート機能（マルウェア対策の署名のアップデートおよびコードベースのアップデートの提供を含む）および KSN 機能は、アメリカ合衆国内にある本ソフトウェアではご利用いただけなくなる可能性があります。

Kaspersky Endpoint Security のリモートインストールの準備

このセクションでは、Kaspersky Security Center の管理者用ワークステーションへの Kaspersky Endpoint Security 管理プラグインのインストールの詳細と、リモートコンピュータへのネットワークエージェントのインストールの詳細を説明します。

Kaspersky Security Center から Kaspersky Endpoint Security をインストールするには、Kaspersky Endpoint Security 管理プラグインとネットワークエージェントをインストールしておく必要があります。

Kaspersky Endpoint Security 管理プラグインをインストールする

Kaspersky Endpoint Security 管理プラグインは、管理コンソールから Kaspersky Endpoint Security を管理するためのインターフェイスを提供します。

[Kaspersky Endpoint Security 管理プラグインをインストールする](#)

- Kaspersky Security Center の管理者用ワークステーションで、Kaspersky Endpoint Security のインストールパッケージのファイルが含まれる圧縮ファイルを解凍します。
- Kaspersky Endpoint Security インストールパッケージのファイルが含まれたフォルダを開きます。
- klcfginst.exe をダブルクリックします。

Kaspersky Endpoint Security 管理プラグインのインストールが開始します。

重要：Kaspersky Endpoint Security 管理プラグインをインストールする前に、Kaspersky Security Center の管理者用ワークステーションの管理コンソールを閉じてください。

ローカルでネットワークエージェントをインストールする

ローカルでネットワークエージェントをインストールする

1. リモートコンピュータで、ネットワークエージェントの配布キットのフォルダを開きます。
2. ネットワークエージェントの配布キット（DMG ファイル）を開きます。
配布キットの内容が表示されたウィンドウが開きます。
3. 配布キットの内容のウィンドウで、**[ネットワークエージェント]** をダブルクリックします。
4. **[続行]** をクリックして、ネットワークエージェントをインストールすることを確認します。
5. **[はじめに]** ウィンドウで、**[続行]** をクリックします。
6. **[ライセンス]** ウィンドウで、お客様と AO Kaspersky Lab との間で交わされるネットワークエージェントの使用許諾契約書を読み、次の操作を実行します：
 - 使用許諾契約書のすべての条項に同意する場合は、**[続行]** をクリックします。
 - 使用許諾契約書のテキストを印刷する場合は、**[プリント]** をクリックします。
 - 使用許諾契約書をテキストファイルとして保存する場合は、**[保存]** をクリックします。
7. 確認ウィンドウで、次のいずれかを選択します：
 - ネットワークエージェントのインストールを続行するには、**[同意する]** をクリックします。
 - 使用許諾契約書をもう一度お読みになる場合は、**[使用許諾契約書を読む]** をクリックします。
 - インストールをキャンセルする場合は、**[同意しない]** をクリックします。
8. **[設定]** ウィンドウで、次の操作を実行します：
 - a. **[サーバ]** に、Kaspersky Security Center がインストールされているサーバの IP アドレスまたは DNS 名を指定します。
 - b. **[ポート]** に、サーバへの暗号化されていない接続で使用するポート番号を指定します。
 - c. **[SSL ポート]** に、サーバへの SSL 接続で使用するポート番号を指定します。
 - d. ネットワークエージェントをインストール後すぐに起動するには、**[インストール後に実行する]** をオンにします。サーバとの接続に SSL を使用しない場合は、**[SSL を使用する]** をオフにします。インストールを続行するには、**[続行]** をクリックします。
9. **[インストールの種類]** ウィンドウで、ネットワークエージェントのインストール先となるディスクに関する情報を読みます。
推奨の設定でネットワークエージェントをインストールするには、**[インストール]** をクリックして、管理者のパスワードを入力し、選択したインストールの種類を確認します。
ネットワークエージェントのインストーラが製品のコンポーネントをインストールし終わるまで待ちます。
10. **[閉じる]** をクリックして、インストーラを終了します。

Apple Remote Desktop を使用してネットワークエージェントをインストールする

1. リモートコンピュータで、**[Apple メニュー]** → **[システム設定]** → **[一般]** → **[共有]** の順に選択します。
2. **[リモートマネージメント]** をオンにします。
3. サーバとして使用する Mac に、Apple Remote Desktop をインストールします。Apple Remote Desktop の詳細は、[Apple のサポートサイト](#)  を参照してください。
4. Apple Remote Desktop を開きます。
5. **[Remote Desktop]** ウィンドウで、左側の **[スキャナ]** をクリックし、ネットワークエージェントをインストールするデバイスを選択します。
6. **[コピー]** をクリックします。
7. **+** をクリックし、ネットワークエージェントのインストールファイル（DMG ファイル、KUD ファイル、SH ファイル）を選択します。

8. [項目の保存場所] ポップアップメニューで、**ディスクの最上位フォルダ**を選択します。
9. [コピー] をクリックします。
10. ファイルのコピー後、[Unix] をクリックします。
11. 次のコマンドを入力します：

```
cd /;  
./install.sh --accept_eula -r <管理サーバーアドレス>
```

<管理サーバーアドレス> は、Kaspersky Security Center 管理サーバーの DNS 名または IP アドレスです。

注意：このコマンドを入力すると、使用許諾契約書に同意したことになります。

12. コマンドを**ユーザ**として実行することを選択し、フィールドに「root」と入力します。
 13. [送信] をクリックします。
- 選択したデバイスへのネットワークエージェントのインストールが開始されます。

Kaspersky Security Center を使用してネットワークエージェントをインストールする

Kaspersky Security Center は、SSH 接続を使用してクライアントコンピュータにネットワークエージェントをインストールします。

クライアントコンピュータにネットワークエージェントをインストールする前に、次の条件が満たされていることを確認してください：

- Kaspersky Security Center 管理サーバーが企業ネットワークに導入されている。
- Kaspersky Security Center の管理者用ワークステーションに管理コンソールがインストールされている。
- リモートコンピュータでリモートログインが有効になっている。
- リモートインストールタスクの実行に使用する専用の管理者アカウントがリモートコンピュータで作成されている。インストールにはドメインアカウントを使用できます。
- 専用アカウントに対して `sudo` のパスワードが無効になっている。

ネットワークエージェントのインストールパッケージの作成

1. Kaspersky Security Center の管理コンソールを起動します。
2. [管理サーバー-<サーバー名>] フォルダを展開します。
3. コンソールツリーで [詳細] フォルダの [リモートインストール] サブフォルダを選択して、[インストールパッケージ] サブフォルダを選択します。
4. 作業領域で [インストールパッケージの作成] をクリックします。
5. [インストールパッケージの種別の選択] ウィンドウで、[カスペルスキー製品のインストールパッケージを作成する] をクリックします。
6. [インストールパッケージ名の定義] ウィンドウで、[名前] に新しいインストールパッケージの名前を入力し、[次へ] をクリックします。
7. [インストールする配布パッケージの選択] ウィンドウで、[参照] をクリックします。
インストールパッケージを作成するためのファイルを選択するウィンドウが表示されます。
8. ネットワークエージェントのインストールパッケージが含まれたフォルダを開いて、`klagent.kud` ファイルを選択します。
[インストールする配布パッケージの選択] ウィンドウに、追加したファイルを使用してリモートでインストールするアプリケーションの名前とバージョンが表示されます。
9. [次へ] をクリックします。
指定された設定で、Kaspersky Endpoint Security のインストールパッケージが作成されます。
10. ウィザードの最後のウィンドウで [終了] をクリックして、新規パッケージウィザードを終了します。

クライアントコンピュータにネットワークエージェントをリモートでインストールするタスクを作成する

1. Kaspersky Security Center の管理コンソールを起動します。
2. [管理サーバー-<サーバー名>] フォルダを展開します。
3. [タスク] フォルダを選択します。
4. 作業領域で、[新規タスク] をクリックして、新規タスクウィザードを開始します。
5. 新規タスクウィザードの手順に従って、クライアントコンピュータにリモートで Kaspersky Endpoint Security をインストールするタスクを作成します。

ウィザードの次の手順に進むには、[次へ] をクリックします。ウィザードの前の手順に戻るには、← をクリックします。ウィザードを途中で停止するには、[キャンセル] をクリックします。

注意： ボタンの外観は、Windows のバージョンによって異なる場合があります。

ステップ1：タスク種別の選択

1. [タスク種別の選択] ウィンドウで、[Kaspersky Security Center 管理サーバー] フォルダを展開します。
2. [アプリケーションのリモートインストール] タスクを選択します。

ステップ2：インストールパッケージの選択

[インストールパッケージの選択] ウィンドウで、次のいずれかを実行します：

- ネットワークエージェントのインストールパッケージで、必要な設定が指定されているものが以前に作成されている場合は、[インストールパッケージの選択] ウィンドウの上部にあるインストールパッケージのリストから該当するインストールパッケージを選択します。
- 必要なインストールパッケージがまだ作成されていない場合は、[新規] をクリックして新規パッケージウィザードを起動します。

ステップ3：インストールの設定

[設定] ウィンドウで、次の操作を実行します：

1. [管理サーバーを通じてオペレーティングシステムの共有フォルダを使用する] をオンにします。
2. 他のすべてのチェックボックスをオフにします。

ステップ4：インストール後にコンピュータの移動先となる管理グループの選択

必要に応じて、[管理対象デバイスをリストへ移動] ウィンドウで、インストール後のコンピュータの移動先となるグループを選択します。

ステップ5：タスクを割り当てるデバイスの選択方法を指定

[タスクを割り当てるデバイスの選択] ウィンドウで、クライアントコンピュータの指定方法を選択します：

- 管理サーバーがネットワークで検出したコンピュータの中から選択する場合は、[ネットワークの管理サーバーによって検出されたデバイスを選択する] を選択します。
- コンピュータの IP アドレスを手動で指定するか、ファイルからコンピュータの IP アドレスをインポートする場合は、[デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする] を選択します。
- 事前に設定された基準に基づいてデバイスを選択するタスクを作成する場合は、[デバイスの抽出にタスクを割り当てる] を選択します。
- 特定の管理グループのコンピュータを選択する場合は、[管理グループにタスクを割り当てる] を選択します。

ステップ6：クライアントコンピュータの選択

表示されるウィンドウで（前のステップで選択したオプションに応じて、[デバイスの選択]、[デバイスの抽出]、[管理グループの選択]のいずれかが表示されます）、クライアントコンピュータの選択、コンピュータの IP アドレスの指定、コンピュータの抽出条件の指定、またはタスクを適用する管理グループの選択を行います。

ステップ7: タスクを実行するアカウントの選択

1. [タスクを実行するアカウントの選択] ウィンドウで、[アカウントが必要(ネットワークエージェントの使用なし)] をオンにします。
2. [追加] → [アカウント] の順にクリックします。
[アカウント] ウィンドウが表示されます。
3. リモートコンピュータの専用管理者アカウントのログイン名とパスワードを指定します。
4. [OK] をクリックします。

ステップ8: タスクスケジュールの設定

1. [タスクスケジュールの設定] ウィンドウで、[実行予定] ドロップダウンリストから起動方法を選択します。
2. 必要に応じて、タスクの自動起動スケジュールを（タスクの起動日時を指定して）設定します。
3. アプリケーションがスケジュールに従って起動できない場合（たとえば、スケジュールされた時間にコンピュータの電源がオフであるなど）にタスクを実行する場合は、[未実行のタスクを実行する] をオンにします。
タスクの開始を妨げている障害が取り除かれ次第、タスクを開始します。

ステップ9: タスク名の指定

[タスク名の定義] ウィンドウの [名前] に、作成するタスクの名前を入力します。

ステップ10: タスクの作成終了

[タスク作成の完了] ウィンドウで、次の操作を実行します：

1. ウィザード終了後にすぐにタスクを開始するには、[ウィザード完了後にタスクを実行する] をオンにします。
2. [完了] をクリックして、ウィザードを終了します。

SSH プロトコルを使用してネットワークエージェントをインストールする

リモートコンピュータにネットワークエージェントをインストールする方法として、SSH プロトコルを使用する方法があります。

次の前提条件を満たしていることを確認してください：

- Kaspersky Security Center 管理サーバーが企業ネットワークに導入されている。
- Kaspersky Security Center の管理者用ワークステーションに管理コンソールがインストールされている。
- ネットワークエージェントのインストールパッケージが作成され、管理サーバーの共有フォルダに保存されている。
- リモートコンピュータでリモートログインが有効になっている。
- ネットワークエージェントのインストールに使用するコンピュータアカウントが `sudoers` に含まれている。

インストールパッケージの詳細は、[Kaspersky Security Center のヘルプ !\[\]\(c80134b111ceae9172eafdd3a547dc96_img.jpg\)](#) を参照してください。

SSH プロトコルを使用してネットワークエージェントをインストールする

1. 管理者のワークステーションで SSH クライアントを起動します。
2. リモートコンピュータに接続します。

3. 管理サーバーの共有フォルダを、リモートコンピュータのネットワークドライブとして接続します。これには、SSH クライアントに次のコマンドを入力します：

```
mkdir /Volumes/KLSHARE
mount_smbfs //<管理者アカウント>:<パスワード>@<管理サーバーの IP アドレス>/KLSHARE /Volumes/KLSHARE
```

パラメータの説明：

- ・ <管理者アカウント> - 管理サーバーの管理者アカウントの名前。
- ・ <パスワード> - 管理サーバーの管理者のパスワード。
- ・ <管理サーバーの IP アドレス> - Kaspersky Security Center を運用しているサーバの IP アドレス。

4. インストールスクリプトを実行します。これには、SSH クライアントに次のコマンドを入力します：

```
cd /Volumes/KLSHARE/<klagent_package_folder>
```

<klagent_package_folder> は、ネットワークエージェントのインストールパッケージが格納されているフォルダです。

```
sudo ./install.sh --accept_eula [-r <サーバ>] [-p <ポート番号>] [-s use_ssl 0|1] [-l <SSL ポート番号>] [-x use_proxy 0|1] [-a <プロキシ>] [-n <proxy login>] [-w <proxy password>]
```

パラメータの説明：

- ・ <サーバ> - Kaspersky Security Center がインストールされているサーバの IP アドレスまたは DNS 名。
- ・ <ポート番号> - 管理サーバーへの暗号化されていない接続を確立する時に使用されるポートの番号。既定では、ポート 14000 が使用されます。
- ・ use_ssl 0|1 - ネットワークエージェントと管理サーバとの間で接続を確立する時に、暗号化を使用するかどうかを指定します。値が「0」の場合は、暗号化されていない接続を使用します。値が「1」の場合は、SSL プロトコルを使用して接続を確立します（既定値）。
- ・ <SSL ポート番号> - SSL プロトコルを使用して管理サーバーへの暗号化された接続を確立する時に使用されるポートの番号。既定では、ポート 13000 が使用されます。
- ・ use_proxy 0|1 - インターネット接続時に、プロキシサーバが使用されるかどうかを指定するパラメータ。値が「0」の場合は、プロキシサーバを使用しません。値が「1」の場合は、プロキシサーバを使用して接続を確立します（既定値）。
- ・ <プロキシ> - プロキシサーバの IP アドレスまたは DNS 名を入力します。
- ・ <proxy_login> - プロキシサーバへ接続するためのユーザ名。
- ・ <proxy_password> - プロキシサーバへ接続するためのパスワード。

重要：このコマンドの実行には管理者権限が必要です。

5. リモートコンピュータのネットワークドライブを接続解除します。これには、SSH クライアントに次のコマンドを入力します：

```
umount /Volumes/KLSHARE
```

6. リモートコンピュータ上でネットワークエージェントが問題なく機能するか確認します。これには、SSH クライアントに次のコマンドを入力します：

```
cd /Library/Application\ Support/Kaspersky\ Lab/klagent/Binaries/
sudo ./klagentchk
```

チェックが正常に完了すると、ネットワークエージェントは正しく動作します。

ローカルでネットワークエージェントをアンインストールする

1. リモートコンピュータで、ネットワークエージェントの配布キットのフォルダを開きます。
2. ネットワークエージェントの配布キット（DMG ファイル）を開きます。
配布キットの内容が表示されたウィンドウが開きます。
3. 配布キットの内容のウィンドウで、[ネットワークエージェントアンインストーラ] をダブルクリックします。
4. [はじめに] ウィンドウで、[続行] をクリックします。
5. [情報] ウィンドウで、[削除] をクリックします。
6. 管理者の認証情報の入力画面で管理者の名前とパスワードを入力し、ネットワークエージェントのアンインストールを確定します。
ネットワークエージェントのアンインストールが開始されます。
7. アンインストールの完了の情報を確認し、[終了] をクリックしてアンインストーラを終了します。

ネットワークエージェントがリモートコンピュータからアンインストールされます。

コマンドラインからのネットワークエージェントの管理

このセクションでは、クライアントコンピュータでコマンドラインを使用してネットワークエージェントを管理する方法について説明します。

ネットワークエージェントは、クライアントコンピュータでコマンドラインを使用して停止したり再開することができます。

また、**klmover** ユーティリティを使用して、リモートコンピュータを管理サーバーに手動で接続したり、**klagchk** ユーティリティを使用してリモートコンピュータと管理サーバーとの接続をチェックしたりすることも可能です。

ネットワークエージェントをアンインストールできます。

リモートコンピュータ上のネットワークエージェントの開始または停止

リモートコンピュータ上のネットワークエージェントは、コマンドラインを使用して停止および再開できます。

ネットワークエージェントを停止する

リモートコンピュータのコマンドラインで **unload** コマンドを使用して、**launchctl** ユーティリティを起動します。

コマンドの構文：

```
sudo launchctl unload /Library/LaunchDaemons/com.kaspersky.klnagent.plist
```

ネットワークエージェントを開始する

リモートコンピュータのコマンドラインで **load** コマンドを使用して、**launchctl** ユーティリティを起動します。

コマンドの構文：

```
sudo launchctl load /Library/LaunchDaemons/com.kaspersky.klnagent.plist
```

重要：ネットワークエージェントを停止および開始するには、管理者権限が必要です。

クライアントコンピュータと管理サーバー間の接続の手動確認：Klnagchk ユーティリティ

リモートコンピュータと管理サーバー間の接続を確認する

リモートコンピュータのコマンドラインで **klagchk** ユーティリティを実行します。

klagchk ユーティリティは、ネットワークエージェントのインストールパッケージに含まれています。

ネットワークエージェントのインストールが完了すると、**klagchk** ユーティリティは、**/Library/Application Support/Kaspersky Lab/klagent/Binaries** フォルダに保存されます。

klagchk ユーティリティをコマンドラインから実行すると、指定したパラメータに応じて次の操作が実行されます：

- リモートコンピュータにインストールされているネットワークエージェントと管理サーバー間の接続に対して指定した設定を表示する、またはファイルに保存する。
- ネットワークエージェントの前回の起動以降の統計とユーティリティの実行結果をファイルに保存する、または画面に表示する。
- ネットワークエージェントと管理サーバーとの接続を確立しようとする。
- 接続を確立できない場合、**ICMP** パケットを送信して、管理サーバーがインストールされているコンピュータの状態を確認します。

ユーティリティを実行する前に、コマンドラインで **/Library/Application Support/Kaspersky Lab/klagent/Binaries** に移動してください。

コマンドの構文：

```
sudo ./klagchk [-logfile <ファイル名>] [-sp] [-savecert <証明書ファイルのパス>] [-restart]
```

重要：ユーティリティの実行には管理者権限が必要です。

パラメータの説明

-logfile <ファイル名> - ネットワークエージェントと管理サーバー間の接続設定とユーティリティの実行結果をファイルに保存します。このパラメータが未指定の場合、サーバーの接続設定、実行結果およびエラーメッセージは画面に表示されます。

-sp - プロキシサーバーの認証用パスワードを画面に表示するか、ファイルに保存します。このパラメータは、プロキシサーバーを使用してネットワークエージェントから管理サーバーに接続する場合に使用します。既定では、このパラメータは使用されません。

-savecert <ファイル名> - 管理サーバーへの認証用の証明書を、指定したファイルに保存します。

-restart - ユーティリティの実行完了後に、ネットワークエージェントを再起動します。

例：

```
sudo ./klnagchk -logfile klnagchk.log -sp
```

リモートコンピュータから管理サーバーへの手動接続：Klmover ユーティリティ

[リモートコンピュータを管理サーバーに接続する](#)

リモートコンピュータのコマンドラインで **klmover** ユーティリティを実行します。

klmover ユーティリティは、ネットワークエージェントのインストールパッケージに含まれています。

ネットワークエージェントのインストールが完了すると、**klmover** ユーティリティは、`/Library/Application Support/Kaspersky Lab/klnagent/Binaries` フォルダに保存されます。

klmover ユーティリティをコマンドラインから実行すると、指定したパラメータに応じて次の操作が実行されます：

- 指定したパラメータでネットワークエージェントを管理サーバーに接続する。
- ユーティリティの実行結果をファイルに保存する、または画面に表示する。

ユーティリティを実行する前に、コマンドラインで `/Library/Application Support/Kaspersky Lab/klnagent/Binaries` に移動してください。

コマンドラインの構文：

```
sudo ./klmover [-logfile <ファイル名>] [-address <サーバーのアドレス>] [-pn <ポート番号>] [-ps <SSL ポート番号>] [-noss1] [-cert <証明書ファイルのパス>] [-silent] [-dupfix]
```

重要：ユーティリティの実行には管理者権限が必要です。

パラメータの説明

-logfile <ファイル名> - 実行結果をファイルに保存します。このパラメータが未指定の場合、実行結果とエラーメッセージは画面に表示されます。

-address <サーバアドレス> - ネットワークエージェントが管理サーバーに接続する時に使用するアドレス。サーバーの IP アドレスか DNS 名を指定できます。

注意：このパラメータのコマンドを使用して、リモートコンピュータの接続先の管理サーバーのアドレスを変更することもできます。

-pn <ポート番号> - 管理サーバーへの暗号化されていない接続を確立する時に使用されるポートの番号。既定では、ポート **14000** が使用されます。

-ps <SSL ポート番号> - SSL プロトコルを使用して管理サーバーへの暗号化された接続を確立する時に使用されるポートの番号。既定では、ポート **13000** が使用されます。

-noss1 - 管理サーバーへの暗号化されていない接続を使用します。このパラメータが未指定の場合、暗号化された SSL プロトコルを使用して管理サーバーへのセキュアな接続を確立します。

-cert <証明書ファイルへのパス> - 新しい管理サーバーへのアクセス認証に、指定された証明書を使用します。このパラメータが指定されていない場合、ネットワークエージェントは管理サーバーへの初回接続時に証明書を取得します。

-silent - サイレントモードでユーティリティを実行します。

-dupfix - このパラメータは、ネットワークエージェントがこのヘルプで説明されている方法とは異なる方法でインストールされた場合、たとえば、ネットワークエージェントがインストールされたディスクイメージからリカバリされた場合などに使用されます。ネットワークエージェントの自動的な自己証明が原因で、元のコンピュータや他のコンピュータのアイコンが管理コンソール内に複製される場合は、複製されたコンピュータを再接続してみてください。

注意：klmover ユーティリティを実行する際は、すべてのパラメータに対して値を指定してください。

例：

```
sudo ./klmover -logfile klmover.log -address 192.0.2.12 -ps 13001
```

ネットワークエージェントを使用して管理サーバーに接続されているリモートコンピュータは、クライアントコンピュータと呼ばれます。

ネットワークエージェントをアンインストールする

コマンドの構文：

```
sudo '/Library/Application Support/Kaspersky Lab/klnagent/Binaries/UninstallScript'
```

Kaspersky Endpoint Security のインストールとアンインストール

このセクションでは、Kaspersky Endpoint Security をクライアントコンピュータにリモートでインストールおよびアンインストールする方法について説明します。

[Kaspersky Endpoint Security](#) を、[ローカルでインストールやアンインストールする](#)ことも、[Kaspersky Security Center Web コンソール](#)  や、[Kaspersky Security Center Cloud コンソール](#)  から行うこともできます。

SSH プロトコルを使用したインストール

リモートコンピュータに Kaspersky Endpoint Security をインストールする前に、次の条件が満たされていることを確認してください：

- Kaspersky Security Center 管理サーバーが企業ネットワークに導入されている。
- Kaspersky Security Center の管理者用ワークステーションに管理コンソールがインストールされている。
- Kaspersky Endpoint Security のインストールパッケージが作成され、管理サーバーの共有フォルダに配置されている。
- Kaspersky Endpoint Security のライセンス情報ファイルが管理サーバーの共有フォルダに配置されている（オプション）。
- リモートコンピュータでリモートログインが有効になっている。
- 製品のインストールに使用するコンピュータアカウントが sudoers に含まれている。

[SSH プロトコルを使用してクライアントコンピュータに Kaspersky Endpoint Security をインストールする](#)

1. Kaspersky Security Center の管理者用ワークステーションで SSH クライアントを起動します。
2. リモートコンピュータに接続します。
3. 管理サーバーの共有フォルダを、リモートコンピュータのネットワークドライブとして接続します。これには、SSH クライアントに次のコマンドを入力します：

```
mkdir /Volumes/KLSHARE
```

```
mount_smbfs //<管理者アカウント>:<パスワード>@<管理サーバーの IP アドレス>/KLSHARE /Volumes/KLSHARE
```

パラメータの説明：

- <管理者アカウント> - 管理サーバーの管理者アカウントの名前。
- <パスワード> - 管理サーバーの管理者のパスワード。

- <管理サーバーの IP アドレス> - Kaspersky Security Center を運用しているサーバーの IP アドレス。

4. インストールスクリプトを実行します。これには、SSH クライアントに次のコマンドを入力します：

```
cd /Volumes/KLSHARE/<KES のパッケージフォルダ>  
./install.sh --accept_eula
```

<KES のパッケージフォルダ> は、Kaspersky Endpoint Security のインストールパッケージが格納されているフォルダです。

重要：このコマンドの実行には管理者権限が必要です。

5. リモートコンピュータのネットワークドライブを接続解除します。これには、SSH クライアントに次のコマンドを入力します：

```
umount /Volumes/KLSHARE
```

Kaspersky Security Center を使用したインストール

クライアントコンピュータに Kaspersky Endpoint Security をインストールする前に、次の条件が満たされていることを確認してください：

- Kaspersky Security Center 管理サーバーが企業ネットワークに導入されている。
- Kaspersky Security Center の管理者用ワークステーションに管理コンソールがインストールされている。
- クライアントコンピュータにネットワークエージェントがインストールされている。
- [Kaspersky Endpoint Security のインストールパッケージが作成され](#)、管理サーバーの共有フォルダに保存されている。
- Kaspersky Endpoint Security のライセンス情報ファイルが管理サーバーの共有フォルダに保存されている（オプション）。
- クライアントコンピュータが管理サーバーの「**管理対象コンピューター**」管理グループに追加されている（オプション）。

管理サーバーの管理グループの詳細は、[Kaspersky Security Center のヘルプを](#) 参照してください。

Kaspersky Security Center を使用して、クライアントコンピュータに Kaspersky Endpoint Security をインストールするには、「**アプリケーションのリモートインストール**」タスクを作成して実行する必要があります。

[クライアントコンピュータに Kaspersky Endpoint Security をリモートでインストールするタスクを作成する](#)

1. Kaspersky Security Center の管理コンソールを起動します。
2. 「**管理サーバ - <サーバ名>**」フォルダを展開します。
3. 「**タスク**」フォルダを選択します。
4. 作業領域で、「**新規タスク**」をクリックして、新規タスクウィザードを開始します。
5. 新規タスクウィザードの手順に従って、クライアントコンピュータにリモートで Kaspersky Endpoint Security をインストールするタスクを作成します。

ウィザードの次の手順に進むには、「**次へ**」をクリックします。ウィザードの前の手順に戻るには、**←** をクリックします。ウィザードを途中で停止するには、「**キャンセル**」をクリックします。

注意：ボタンの外観は、Windows のバージョンによって異なる場合があります。

[ステップ1：タスク種別の選択](#)

1. 「**タスク種別の選択**」ウィンドウで、「**Kaspersky Security Center 管理サーバー**」フォルダを展開します。
2. 「**アプリケーションのリモートインストール**」タスクを選択します。

[ステップ2：インストールパッケージの選択](#)

「**インストールパッケージの選択**」ウィンドウで、次のいずれかを実行します：

- Kaspersky Endpoint Security のインストールパッケージで、必要な設定が指定されているものが以前に作成されている場合は、**「インストールパッケージの選択」** ウィンドウの上部にあるインストールパッケージのリストから該当するインストールパッケージを選択します。
- 必要なインストールパッケージがまだ作成されていない場合は、**「新規」** をクリックして [新規パッケージウィザード](#) を起動します。

ステップ3: 追加アプリケーションのインストール

クライアントコンピュータにネットワークエージェントもインストールする場合は、**「詳細」** ウィンドウで、**「このアプリケーションと同時にネットワークエージェントをインストールする」** と **ネットワークエージェントのインストールパッケージ名** のチェックボックスをオンにします。

注意: ネットワークエージェントのインストールパッケージは事前に作成しておく必要があります。まだ作成されていない場合は、**「作成」** をクリックして新規パッケージウィザードを起動します。

ステップ4: インストールの設定

「設定」 ウィンドウで、アプリケーションのリモートインストールを設定します。

ステップ5: インストール後にコンピュータの移動先となる管理グループの選択

必要に応じて、**「管理対象デバイスをリストへ移動」** ウィンドウで、インストール後のコンピュータの移動先となるグループを選択します。

注意: **「管理対象デバイスをリストへ移動」** ウィンドウは、ステップ3でネットワークエージェントのインストールを選択した場合に表示されます。

ステップ6: タスクを割り当てるデバイスの選択方法を指定

「タスクを割り当てるデバイスの選択」 ウィンドウで、クライアントコンピュータの指定方法を選択します：

- 管理サーバーがネットワークで検出したコンピュータの中から選択する場合は、**「ネットワークの管理サーバーによって検出されたデバイスを選択する」** を選択します。
- コンピュータの IP アドレスを手動で指定するか、ファイルからコンピュータの IP アドレスをインポートする場合は、**「デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする」** を選択します。
- 事前に設定された基準に基づいてデバイスを選択するタスクを作成する場合は、**「デバイスの抽出にタスクを割り当てる」** を選択します。
- 特定の管理グループのコンピュータを選択する場合は、**「管理グループにタスクを割り当てる」** を選択します。

ステップ7: クライアントコンピュータの選択

表示されるウィンドウで（前のステップで選択したオプションに応じて、**「デバイスの選択」**、**「デバイスの抽出」**、**「管理グループの選択」** のいずれかが表示されます）、クライアントコンピュータの選択、コンピュータの IP アドレスの指定、コンピュータの抽出条件の指定、またはタスクを適用する管理グループの選択を行います。

ステップ8: タスクを実行するアカウントの選択

「タスクを実行するアカウントの選択」 ウィンドウで、**「アカウントが不要（ネットワークエージェントインストール済み）」** をオンにします。

このウィザードを起動する前にネットワークエージェントがインストール済みであることを前提としています。

ステップ9: タスクスケジュールの設定

1. **「タスクスケジュールの設定」** ウィンドウで、**「実行予定」** ドロップダウンリストから起動方法を選択します。
2. 必要に応じて、タスクの自動起動スケジュールを（タスクの起動日時を指定して）設定します。

3. アプリケーションがスケジュールに従って起動できない場合（たとえば、スケジュールされた時間にコンピュータの電源がオフであるなど）にタスクを実行する場合は、**「未実行のタスクを実行する」** をオンにします。
タスクの開始を妨げている障害が取り除かれ次第、タスクを開始します。

ステップ10：タスク名の指定

「タスク名の定義」 ウィンドウの **「名前」** に、作成するタスクの名前を入力します。

ステップ11：タスクの作成終了

「タスク作成の完了」 ウィンドウで、次の操作を実行します：

1. ウィザード終了後にすぐにタスクを開始するには、**「ウィザード完了後にタスクを実行する」** をオンにします。
2. **「完了」** をクリックして、ウィザードを終了します。

「タスク」 フォルダの作業領域に、作成したタスクが表示されます。

インストールパッケージの作成

「アプリケーションのリモートインストール」 タスクを作成する際、既存のインストールパッケージを使用するか新規のインストールパッケージを作成することができます。作成したインストールパッケージのリストを表示するには、**「詳細」** → **「リモートインストール」** → **「インストールパッケージ」** の順にクリックします。

Kaspersky Security Center でインストールパッケージを作成する

1. Kaspersky Security Center の管理コンソールを起動します。
2. **「管理サーバ - <サーバ名>」** フォルダを展開します。
3. コンソールツリーで **「詳細」** フォルダの **「リモートインストール」** サブフォルダを選択して、**「インストールパッケージ」** サブフォルダを選択します。
4. 作業領域で **「インストールパッケージの作成」** をクリックします。
5. **「インストールパッケージの種別の選択」** ウィンドウで、**「カスペルスキー製品のインストールパッケージを作成する」** をクリックします。
6. **「インストールパッケージ名の定義」** ウィンドウで、**「名前」** に新しいインストールパッケージの名前を入力し、**「次へ」** をクリックします。
7. **「インストールする配布パッケージの選択」** ウィンドウで、**「参照」** をクリックします。
インストールパッケージを作成するためのファイルを選択するウィンドウが表示されます。
8. Kaspersky Endpoint Security インストールパッケージが含まれたフォルダを開いて、ファイル **kesmac.kud** を選択します。
「インストールする配布パッケージの選択」 ウィンドウに、追加したファイルを使用してリモートでインストールするアプリケーションの名前とバージョンが表示されます。
9. 必要に応じて、**「アップデートをリポジトリからインストールパッケージへコピーする」** をオンにして Kaspersky Security Center の保管領域からインストールパッケージにアプリケーションのアップデートをコピーし、**「次へ」** をクリックします。
インストールパッケージの管理サーバーへのアップロードが開始します。アップロードが終了すると、**「インストール種別」** ウィンドウが表示されます。
10. **「インストール種別」** ウィンドウの **「インストールするパッケージ」** セクションで、クライアントコンピュータへのインストールでスキップするコンポーネントの名前に隣接するチェックボックスをオンまたはオフにし、**「次へ」** をクリックします。
指定された設定で、Kaspersky Endpoint Security のインストールパッケージが作成されます。
11. ウィザードの最後のウィンドウで **「終了」** をクリックして、新規パッケージウィザードを終了します。

Kaspersky Security Center を使用したアンインストール

Kaspersky Security Center を使用して、クライアントコンピュータから Kaspersky Endpoint Security を削除する前に、次の条件が満たされていることを確認してください：

- Kaspersky Security Center 管理サーバーが企業ネットワークに導入されている。

- Kaspersky Security Center の管理者用ワークステーションに管理コンソールがインストールされている。
- クライアントコンピュータにネットワークエージェントがインストールされている。

Kaspersky Security Center を使用してクライアントコンピュータから Kaspersky Endpoint Security をアンインストールするには、[アプリケーションのリモートアンインストール] タスクを作成して実行する必要があります。

重要：クライアントコンピュータから Kaspersky Endpoint Security を削除すると、コンピュータが感染する危険性が生じます。

クライアントコンピュータからリモートで Kaspersky Endpoint Security をアンインストールするタスクを作成する

1. Kaspersky Security Center の管理コンソールを起動します。
2. [管理サーバ - <サーバ名>] フォルダを展開します。
3. [タスク] フォルダを選択します。
4. 作業領域で、[新規タスク] をクリックして、新規タスクウィザードを開始します。
5. 新規タスクウィザードの手順に従って、クライアントコンピュータからリモートで Kaspersky Endpoint Security をアンインストールするタスクを作成します。

ウィザードの次の手順に進むには、[次へ] をクリックします。ウィザードの前の手順に戻るには、← をクリックします。ウィザードを途中で停止するには、[キャンセル] をクリックします。

注意：ボタンの外観は、Windows のバージョンによって異なる場合があります。

ステップ 1: タスク種別の選択

1. [タスク種別の選択] ウィンドウで、[Kaspersky Security Center 管理サーバ] フォルダを展開します。
2. [詳細] フォルダを展開します。
3. [アプリケーションのリモートアンインストール] タスクを選択します。

ステップ 2: アンインストールするアプリケーションの選択

[削除するアプリケーションの選択] ウィンドウで、[Kaspersky Security Center に対応するアプリケーションをアンインストールする] を選択します。

ステップ 3: アンインストールの設定

[設定] ウィンドウで、次の操作を実行します：

1. [削除するアプリケーション] ドロップダウンリストから、[Kaspersky Endpoint Security for Mac 12.2] を選択します。
2. [次へ] をクリックします。
3. アプリケーションのリモートアンインストールを設定します。

ステップ 4: オペレーティングシステムの再起動方法の選択

[オペレーティングシステムの再起動のオプションを選択] ウィンドウで、[デバイスを再起動しない] を選択します。

ステップ 5: タスクを割り当てるデバイスの選択

[タスクを割り当てるデバイスの選択] ウィンドウで、クライアントコンピュータの指定方法を選択します：

- 管理サーバーがネットワークで検出したコンピュータの中から選択する場合は、**「ネットワークの管理サーバーによって検出されたデバイスを選択する」**を選択します。
- コンピュータの IP アドレスを手動で指定するか、ファイルからコンピュータの IP アドレスをインポートする場合は、**「デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする」**を選択します。
- 事前に設定された基準に基づいてデバイスを選択するタスクを作成する場合は、**「デバイスの抽出にタスクを割り当てる」**を選択します。
- 特定の管理グループのコンピュータを選択する場合は、**「管理グループにタスクを割り当てる」**を選択します。

ステップ6: クライアントコンピュータの選択

表示されるウィンドウで（前のステップで選択したオプションに応じて、**「デバイスの選択」**、**「デバイスの抽出」**、**「管理グループの選択」**のいずれかが表示されます）、クライアントコンピュータの選択、コンピュータの IP アドレスの指定、コンピュータの抽出条件の指定、またはタスクを適用する管理グループの選択を行います。

ステップ7: タスクを実行するユーザアカウントの選択

「タスクを実行するアカウントの選択」 ウィンドウで、**「アカウントが不要（ネットワークエージェントインストール済み）」**をオンにします。

このウィザードを起動する前にネットワークエージェントがインストール済みであることを前提としています。

ステップ8: タスクスケジュールの設定

1. **「タスクスケジュールの設定」** ウィンドウで、**「実行予定」** ドロップダウンリストから起動方法を選択します。
2. 必要に応じて、タスクの自動起動スケジュールを（タスクの起動日時を指定して）設定します。
3. アプリケーションがスケジュールに従って起動できない場合（たとえば、スケジュールされた時間にコンピュータの電源がオフであるなど）にタスクを実行する場合は、**「未実行のタスクを実行する」**をオンにします。
タスクの開始を妨げている障害が取り除かれ次第、タスクを開始します。

ステップ9: タスク名の指定

「タスク名の定義」 ウィンドウの **「名前」** に、作成するタスクの名前を入力します。

ステップ10: タスクの作成終了

「タスク作成の完了」 ウィンドウで、次の操作を実行します：

1. ウィザード終了後にすぐにタスクを開始するには、**「ウィザード完了後にタスクを実行する」**をオンにします。
2. **「完了」** をクリックして、ウィザードを終了します。

「タスク」 フォルダの作業領域に、作成したタスクが表示されます。

Kaspersky Security Center からの製品の開始と停止

Kaspersky Security Center で管理しているデバイスのリストから選択したコンピュータで Kaspersky Endpoint Security を開始または停止できます。

Kaspersky Security Center から Kaspersky Endpoint Security を開始または停止する

1. Kaspersky Security Center の管理コンソールを起動します。
2. **「管理サーバー - <サーバー名>」** フォルダを展開します。
3. コンソールツリーで、**「管理対象デバイス」** をクリックします。
4. 対象のクライアントコンピュータが含まれた管理グループを選択します。

5. **［デバイス］** タブを選択します。
6. クライアントコンピュータのリストからコンピュータを選択します。
7. 次のいずれかの方法で、**プロパティ**：<**コンピュータ名**>ウインドウを開きます：
 - クライアントコンピュータの名前をダブルクリックする。
 - クライアントコンピュータを右クリックして、コンテキストメニュー **［プロパティ］** を選択する。
8. **［アプリケーション］** セクションを選択します。
9. **［このデバイスにインストール済みのカスペルスキー製品］** リストで、**［Kaspersky Endpoint Security for Mac 12.2］** を右クリックしてコンテキストメニューを開き、次のいずれかを実行します：
 - **［開始］** を選択すると、アプリケーションが開始されます。
 - **［停止］** を選択すると、アプリケーションが停止されます。

重要：Kaspersky Endpoint Security が停止すると、クライアントコンピュータは保護されていない状態で稼働し続けるため、感染する危険性が生じます。

タスクの作成と管理

このセクションでは、クライアントコンピュータまたはコンピュータグループに対して実施する Kaspersky Endpoint Security のタスクを、Kaspersky Security Center を使用して作成および設定する方法について説明します。

タスクとは、Kaspersky Endpoint Security がクライアントコンピュータで実行する、設定可能な処理のセットのことです。

Kaspersky Security Center では次のタスクを作成できます：

- ライセンスの追加
- 簡易スキャン
- ロールバック
- スキャン
- アップデート

タスクに対して実行可能な操作は次の通りです：

- タスクの開始と停止。
- タスク設定の編集。
- タスクの進行状況の追跡。
- あるグループから別のグループへのタスクのコピーおよび移動。
- タスクの削除。
- タスクのインポートおよびエクスポート。

タスクの詳細は、[Kaspersky Security Center のヘルプ](#)  を参照してください。

タスクの作成

Kaspersky Security Center から Kaspersky Endpoint Security を管理する場合、次の種別のタスクを作成できます：

- ローカルタスク：ローカルタスクとは、別のクライアントコンピュータで実行することを目的に作成されたタスクを意味します。
- グループタスク：グループタスクとは、管理グループのコンピュータで実行されるタスクを意味します。
- 任意のコンピュータに対するタスク：任意のコンピュータで実行するタスクを作成できます。対象となるコンピュータが管理コンピュータやコンピュータの抽出条件に属しているかどうかは考慮されません。

[別のクライアントコンピュータ向けのローカルタスクの作成](#) 

1. Kaspersky Security Center の管理コンソールを起動します。
2. [管理サーバ - <サーバ名>] フォルダを展開します。
3. コンソールツリーで、[管理対象デバイス] をクリックします。
4. 対象のクライアントコンピュータが含まれた管理グループを選択します。
5. 作業領域で、[デバイス] タブを選択します。
6. クライアントコンピュータのリストからコンピュータを選択します。
7. 次のいずれかの方法で、プロパティ：<コンピュータ名> ウィンドウを開きます：
 - クライアントコンピュータの名前をダブルクリックする。
 - クライアントコンピュータを右クリックして、コンテキストメニュー [プロパティ] を選択する。
8. プロパティ：<コンピュータ名> ウィンドウで、[タスク] セクションを選択します。
作業領域の右側に、選択したクライアントコンピュータのシステムタスクとカスタムタスクのリストが表示されます。
9. 作業領域の下部にある [追加] をクリックします。
新規タスクウィザードが起動します。
10. 新規タスクウィザードの手順に従って、別のクライアントコンピュータ向けのローカルタスクを作成します。

管理グループのクライアントコンピュータ向けのタスクを作成する

1. Kaspersky Security Center の管理コンソールを起動します。
2. [管理サーバ - <サーバ名>] フォルダを展開します。
3. コンソールツリーで、[管理対象デバイス] をクリックします。
4. 対象のクライアントコンピュータが含まれた管理グループを選択します。
5. 作業領域で、[タスク] タブを選択します。
6. 作業領域で、[新規タスク] をクリックして、新規タスクウィザードを開始します。
7. 新規タスクウィザードの手順に従って、管理グループに含まれるクライアントコンピュータ向けのタスクを作成します。

グループタスクの作成方法の詳細は、[Kaspersky Security Center のヘルプ](#)  を参照してください。

任意のコンピュータに対してタスクを作成する

1. Kaspersky Security Center の管理コンソールを起動します。
2. [管理サーバ - <サーバ名>] フォルダを展開します。
3. コンソールツリーで、[タスク] をクリックします。
4. 作業領域で、[新規タスク] をクリックして、新規タスクウィザードを開始します。
5. 新規タスクウィザードの手順に従って、任意のコンピュータ用のタスクを作成します。

ウィザードの次の手順に進むには、[次へ] をクリックします。ウィザードの前の手順に戻るには、← をクリックします。ウィザードを途中で停止するには、[キャンセル] をクリックします。

注意： ボタンの外観は、Windows のバージョンによって異なる場合があります。

ステップ1: アプリケーションの選択とタスク種別の定義

1. **〔タスク種別の選択〕** ウィンドウで、**〔Kaspersky Endpoint Security for Mac 12.2〕** ノードを展開します。

2. 作成するタスクの種別を選択します：

- ライセンスを追加するタスクを作成する場合は、**〔ライセンスの追加〕** を選択します。
- 簡易スキャンタスクを作成する場合は、**〔簡易スキャン〕** を選択します。
- 最新のアップデートをロールバックするタスクを作成する場合は、**〔ロールバック〕** を選択します。
- マルウェアスキャンタスクを作成するには、**〔スキャン〕** を選択します。
- アップデートタスクを作成する場合は、**〔アップデート〕** を選択します。

ステップ2：選択したタスク種別の設定

設定ウィンドウの内容は、前の手順で選択したタスク種別によって異なります。このウィンドウは、ロールバックタスクでは表示されません。

製品のアクティベーション

〔製品のアクティベーション〕 ウィンドウで、次の操作を実行します：

1. **Kaspersky Security Center** の保管領域からアクティベーションコードまたはライセンス情報ファイルを選択するか、コンピュータに保存したライセンス情報ファイルを追加します。
2. 指定したライセンスを予備のライセンスとして追加するには、**〔予備のライセンスとして追加〕** をオンにします。
現在のライセンスの有効期間が終了すると、予備のライセンスがアクティブになります。

指定されたライセンスに関する情報（ライセンス、ライセンスの種別、ライセンスの有効期限）が、**〔製品のアクティベーション〕** ウィンドウに表示されます。

アップデート

カスペルスキーのアップデートサーバが、**Kaspersky Endpoint Security** のアップデートの主な入手元です。アップデート元には、ディストリビューションポイント、ローカルフォルダおよびその他の **Web** サーバを使用することもできます。

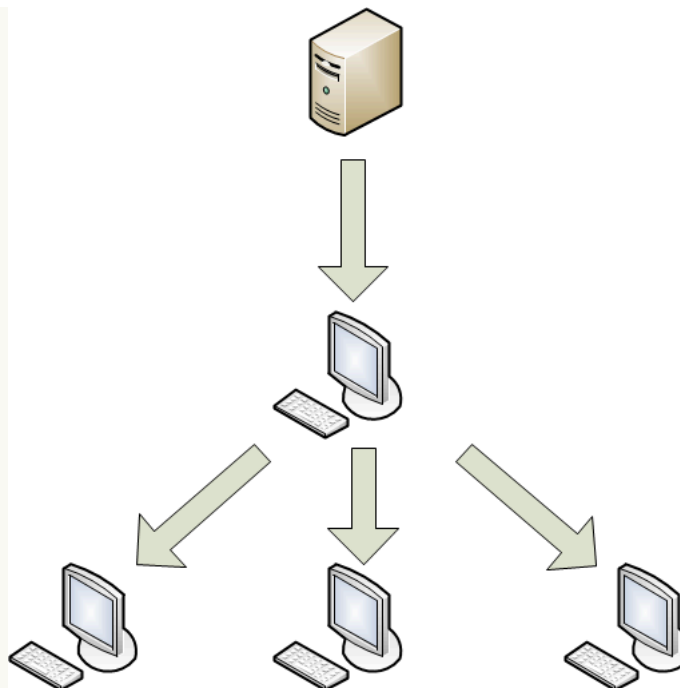
ローカルのフォルダにダウンロードしたアップデートを使用して、企業ネットワーク上の他のコンピュータの **Kaspersky Endpoint Security** の定義データベースとモジュールをアップデートすることにより、インターネットのトラフィック量を削減できます。

次のようにアップデートの配信を設定できます：

1. ネットワーク上のコンピュータのうちの1台がカスペルスキーのアップデートサーバまたは別のアップデート元から **Kaspersky Endpoint Security** のアップデートパッケージを取得します。取得したアップデートは、ローカルの共有フォルダに配置されます。

注意：ローカルの共有フォルダは、あらかじめ作成しておく必要があります。

2. ネットワーク上の他のコンピュータは、ローカルの共有フォルダをアップデート元として参照します。



ローカルコンピュータへのアップデートの配信

必要に応じて、**「アップデート」** ウィンドウで、アップデートタスクの設定を編集します：

1. ソフトウェアモジュールのアップデートを無効にするには、**「ソフトウェアモジュールをアップデートする」** をオフにします。
2. アップデート元を変更するには：
 - a. **「設定」** をクリックします。
「設定：アップデート」 ウィンドウが表示されます。
 - b. 使用するアップデート元に隣接するチェックボックスをオンにします。
3. 別のアップデート元を指定するには、**「追加」** をクリックします。
「アップデート元」 ウィンドウが表示されます。
 - a. アップデート元の URL か、ローカルフォルダまたはネットワークフォルダのパスを指定し、**「OK」** をクリックします。
 - b. **「OK」** をクリックして変更を保存し、**「設定：アップデート」** ウィンドウを閉じます。

スキャンと簡易スキャン

既定では、**「推奨」** のセキュリティレベルを使用します。このレベルは、感染したオブジェクトを検知すると、スキャン後にユーザーに処理の選択を要求するメッセージを表示し、次のオブジェクトをスキャンします：

- すべてのリムーバブルドライブ
- すべての内部ディスク
- すべてのネットワークドライブ
- メモリ

注意：Kaspersky Endpoint Security は、OneDrive や iCloud ストレージ、その他のクラウドストレージにあるファイルをスキャンしません。これらのファイルをスキャン範囲から除外してください。そうしないと、スキャンタスクが「感染したファイルが削除されませんでした」というエラーで終了する可能性があります。

必要に応じて、**「スキャン」** ウィンドウでスキャンの設定を編集します：

1. 事前に設定されたセキュリティレベルのいずれかを選択するか、セキュリティの設定を手動で編集する。
2. 感染したオブジェクトの検知時に Kaspersky Endpoint Security が実行する処理を指定します。
3. スキャン範囲を定義します。

ステップ3: タスクを割り当てるデバイスの選択

注意: このステップは、ローカルタスクおよびグループタスクには該当しません。

「**タスクを割り当てるデバイスの選択**」ウィンドウで、クライアントコンピュータの指定方法を選択します：

- 管理サーバーがネットワークで検出したコンピュータの中から選択する場合は、「**ネットワークの管理サーバーによって検出されたデバイスを選択する**」を選択します。
- コンピュータの IP アドレスを手動で指定するか、ファイルからコンピュータの IP アドレスをインポートする場合は、「**デバイスのアドレスを手動で指定するか、リストからアドレスをインポートする**」を選択します。
- 事前に設定された基準に基づいてデバイスを選択するタスクを作成する場合は、「**デバイスの抽出にタスクを割り当てる**」を選択します。
- 特定の管理グループのコンピュータを選択する場合は、「**管理グループにタスクを割り当てる**」を選択します。

ステップ4: クライアントコンピュータの選択

注意: このステップは、ローカルタスクおよびグループタスクには該当しません。

表示されるウィンドウで（前のステップで選択したオプションに応じて、「**デバイスの選択**」、「**デバイスの抽出**」、「**管理グループの選択**」のいずれかが表示されます）、クライアントコンピュータの選択、コンピュータの IP アドレスの指定、コンピュータの抽出条件の指定、またはタスクを適用する管理グループの選択を行います。

ステップ5: タスクスケジュールの設定

1. 「**タスクスケジュールの設定**」ウィンドウで、「**実行予定**」ドロップダウンリストから起動方法を選択します。
2. 必要に応じて、タスクの自動起動スケジュールを（タスクの起動日時を指定して）設定します。
3. アプリケーションがスケジュールに従って起動できない場合（たとえば、スケジュールされた時間にコンピュータの電源がオフであるなど）にタスクを実行する場合は、「**未実行のタスクを実行する**」をオンにします。
タスクの開始を妨げている障害が取り除かれ次第、タスクを開始します。
4. 各コンピュータでタスクが起動される間隔を自動的に定義するには、「**タスクの開始を自動的かつランダムに遅延させる**」をオンにします。
これにより、Kaspersky Security Center 管理サーバーへの負荷を軽減できます。
5. 各コンピュータでタスクが起動される間隔を指定するには、「**タスクの開始を次の時間範囲内でランダムに遅延させる(分):**」をオンにして、時間を分単位で指定します。
これにより、Kaspersky Security Center 管理サーバーへの負荷を軽減できます。

ステップ6: タスク名の指定

「**タスク名の定義**」ウィンドウの「**名前**」に、作成するタスクの名前を入力します。

ステップ7: タスクの作成終了

「**タスク作成の完了**」ウィンドウで、次の操作を実行します：

1. ウィザード終了後にすぐにタスクを開始するには、「**ウィザード完了後にタスクを実行する**」をオンにします。
2. 「**完了**」をクリックして、ウィザードを終了します。

タスクの手動での開始と停止

スケジュールされたタスクは、スケジュールに従って自動で開始および停止します。ただし、タスクはいつでも手動で開始することができます。

注意：ネットワークエージェントが実行されている場合のみ、クライアントコンピュータでタスクが開始されます。ネットワークエージェントが停止すると、アクティブなタスクの実行がすべて中断されます。

[タスクの手動での開始と停止](#)

1. 開始または停止するタスクが含まれるタスクのリストを表示します。
2. このリストから、開始または停止するタスクを選択します。
3. 次のいずれかの方法で、タスクを開始または停止します：
 - タスクを右クリックしてコンテキストメニューを表示し、**開始** または **停止** を選択します。
 - 作業領域で、**開始** または **停止** をクリックします。
 - タスクを右クリックしてコンテキストメニューを表示し、**プロパティ** を選択します。表示されるウインドウで、**開始** または **停止** をクリックします。

タスクのインポートおよびエクスポート

グループタスクおよび特定のコンピュータに対するタスクをファイルにエクスポートできます。

[タスクをエクスポートする](#)

1. エクスポートするタスクが含まれるタスクのリストを選択します：
 - 管理グループを選択して **タスク** タブを開きます。
 - コンソールツリーで、**タスク** をクリックします。
2. エクスポートするタスクを右クリックして、ショートカットメニューで **すべてのタスク** → **エクスポート** を選択します。
3. **名前を付けて保存** ウインドウで、ファイル名とエクスポートするタスクの保存先を指定します。
4. **保存** をクリックします。

[タスクをインポートする](#)

1. タスクのインポート先となるタスクリストを選択します：
 - 管理グループを選択して **タスク** タブを開きます。
 - コンソールツリーで、**タスク** をクリックします。
 2. 次のいずれかの方法で、タスクをインポートします：
 - タスクリストのショートカットメニューで、**すべてのタスク** → **インポート** の順に選択します。
 - **タスクをファイルからインポート** をクリックします。
 3. **開く** ウインドウで、インポートするタスクファイルのパスを指定します。
 4. **開く** をクリックします。
- タスクリストにタスクが表示されます。

タスクの表示

特定のコンピュータや特定の管理グループのコンピュータ用に作成したタスクのリストや、ローカルタスク以外のすべてのタスクのリストを表示できます。

[特定の管理グループのタスクを表示する](#)

1. Kaspersky Security Center の管理コンソールを起動します。
 2. [管理サーバ - <サーバ名>] フォルダを展開します。
 3. コンソールツリーで、[管理対象デバイス] をクリックします。
 4. 対象のクライアントコンピュータが含まれた管理グループを選択します。
 5. 作業領域で、[タスク] タブを選択します。
- 選択した管理グループのコンピュータ用のタスクリストが表示されます。

[ローカルタスクを表示する](#)

1. Kaspersky Security Center の管理コンソールを起動します。
 2. [管理サーバ - <サーバ名>] フォルダを展開します。
 3. コンソールツリーで、[管理対象デバイス] をクリックします。
 4. 対象のクライアントコンピュータが含まれた管理グループを選択します。
 5. 作業領域で、[デバイス] タブを選択します。
 6. クライアントコンピュータのリストからコンピュータを選択します。
 7. 次のいずれかの方法で、プロパティ：<コンピュータ名> ウィンドウを開きます：
 - クライアントコンピュータの名前をダブルクリックする。
 - クライアントコンピュータを右クリックして、コンテキストメニュー [プロパティ] を選択する。
 8. プロパティ：<コンピュータ名> ウィンドウで、[タスク] セクションを選択します。
- 作業領域の右側に、選択したクライアントコンピュータのシステムタスクとカスタムタスクのリストが表示されます。

[ローカル以外のタスクの表示](#)

1. Kaspersky Security Center の管理コンソールを起動します。
 2. [管理サーバ - <サーバ名>] フォルダを展開します。
 3. コンソールツリーで、[タスク] をクリックします。
- ローカル以外のタスクのリストが表示されます。タスクの対象のコンピュータは、管理グループに含まれているものと含まれていないものがあります。

タスク固有設定の管理

[ローカルタスクの設定を表示する](#)

1. ローカルタスクのリストを開きます。
2. リストからタスクを選択し、次のいずれかの方法でタスクの設定を開きます：
 - タスク名をダブルクリックします。
 - 右クリックしてタスクのショートカットメニューを表示させ、[プロパティ] を選択します。

[グループタスクの設定を表示する](#)

1. 管理グループのグループタスクのリストを開きます。
2. リストからタスクを選択し、次のいずれかの方法でタスクの設定を開きます：
 - タスク名をダブルクリックします。
 - 右クリックしてタスクのショートカットメニューを表示させ、**「プロパティ」**を選択します。
 - 作業領域の**「タスクの設定」**をクリックします。

ローカル以外のタスクの設定を表示する

1. ローカル以外のタスクのリストを開きます。
2. リストからタスクを選択し、次のいずれかの方法でタスクの設定を開きます：
 - タスク名をダブルクリックします。
 - 右クリックしてタスクのショートカットメニューを表示させ、**「プロパティ」**を選択します。
 - 作業領域の**「タスクの設定」**をクリックします。

タスクの詳細は、[Kaspersky Security Center のヘルプ](#)  を参照してください。

ローカルタスク、グループタスク、任意のコンピュータに対するタスク向け

ライセンスの追加タスクの設定を管理する

1. **「ライセンスの追加」** タスクの設定ウインドウを開きます。
2. **「製品のアクティベーション」** セクションを選択します。
3. 必要に応じて、次のいずれかの方法で別のライセンスを追加します：
 - Kaspersky Security Center の保管領域に追加したアクティベーションコードから、ライセンスまたはアクティベーションコードを選択するには：
 - a. **「ライセンスまたはアクティベーションコード」** を選択します。
 - b. **「参照」** をクリックします。
「Kaspersky Security Center の保管領域内にあるライセンスとアクティベーションコード」 ウインドウが表示されます。
 - c. ライセンスまたはアクティベーションコードを選択します。
 - d. **「OK」** をクリックします。
 - ライセンス情報ファイルを追加するには：
 - a. **「ライセンス情報ファイル」** を選択します。
 - b. **「追加」** をクリックします。
ファイルを選択するウインドウが表示されます。
 - c. ライセンス情報ファイルを選択します。
 - d. **「開く」** をクリックします。

注意：別のライセンスを追加すると、現在のライセンスは削除されます。

4. 指定したライセンスを予備のライセンスとして追加するには、**「予備のライセンスとして追加」** をオンにします。
現在のライセンスの期限が切れると、予備のライセンスがアクティブになります。

注意：予備のライセンスの有効期限は、現在のライセンスの有効期限より後である必要があります。

5. 次のいずれかの方法で、変更を保存します：

- **[適用]** をクリックし、**タスクのプロパティ** ウィンドウが開いたままの状態に変更を保存します。
- **[OK]** をクリックし、変更を保存して**タスクのプロパティ** ウィンドウを閉じます。

簡易スキャンタスクの設定を管理する

1. **[簡易スキャン]** タスクの設定ウィンドウを開きます。

2. **[簡易スキャン]** セクションを選択します。

3. Kaspersky Endpoint Security が簡易スキャンタスクを実行する時のセキュリティレベルを変更するには、**[セキュリティレベル]** セクションで、次のいずれかの操作を実行します：

- スライダーを上下させて、事前に設定されたセキュリティレベルを選択します。
選択できるセキュリティレベルは、次の通りです：
 - **最大の保護**：開いているファイル、保存されているファイル、または実行されているファイルを最大限に監視します。
 - **推奨**：カスペルスキーが推奨する設定に従ってファイルを監視します。
既定ではこのセキュリティレベルが設定されています。
 - **速度重視**：最小限のファイルを監視します。メモリリソースを大量に必要とするアプリケーションを快適に使用したい場合は、このセキュリティレベルを選択してください。
- セキュリティの設定を手動で編集します：
 - a. **[設定]** をクリックします。
[設定：スキャン] ウィンドウが表示されます。
 - b. **[全般]** タブの **[ファイル種別]** セクションで、簡易スキャンタスクの実行時にスキャンするファイルの種別を選択します。
 - c. **[全般]** タブの **[最適化]** セクションで、スキャンパフォーマンスを設定します。
 - d. **[全般]** タブの **[複合ファイル]** セクションで、検知するオブジェクトとして分析する複合ファイルを選択します。
 - e. **[詳細]** タブの **[詳細設定]** セクションで、iSwift の使用、およびアプリケーションの統計で検知された悪意のあるオブジェクトに関する情報の記録について設定します。
 - f. **[詳細]** タブの **[ヒューリスティックアナライザー]** セクションで、ヒューリスティック分析の使用を設定し、マルウェアスキャンの際にヒューリスティック分析によって適用される保護レベルを選択します。
 - g. **[OK]** をクリックして変更を保存し、**[設定：スキャン]** ウィンドウを閉じます。
セキュリティレベルが **[カスタム]** に変更されます。
- 既定の設定に戻すには、**[既定]** をクリックします。
セキュリティレベルが **[推奨]** に変更されます。

4. 必要に応じて、**[処理]** セクションで、感染したオブジェクトの検知時に実行する処理を選択します。

5. スキャン範囲を指定するには、**[スキャン範囲]** セクションで **[設定]** をクリックし、**[スキャン範囲]** ウィンドウが開いたら次の操作を実行します：

- a. コンピュータのメモリをスキャンする場合は、**[メモリ]** をオンにします。
- b. スタートアップオブジェクトをスキャンする場合は、**[ログイン項目]** をオンにします。
- c. 他のファイルやフォルダをスキャンする場合は、**[追加]** をクリックして、ファイル、フォルダ、またはファイル名やフォルダ名のマスクを指定します。
- d. **[OK]** をクリックして変更を保存し、**[スキャン範囲]** ウィンドウを閉じます。

6. 次のいずれかの方法で、変更を保存します：

- **[適用]** をクリックし、**タスクのプロパティ** ウィンドウが開いたままの状態に変更を保存します。

- [OK] をクリックし、変更を保存して**タスクのプロパティ**ウィンドウを閉じます。

スキャンタスクの設定を管理する ?

1. スキャンタスクの設定ウィンドウを開きます。
2. [スキャン] セクションを選択します。
3. Kaspersky Endpoint Security がスキャンタスクを実行する時のセキュリティレベルを変更するには、[セキュリティレベル] セクションで、次のいずれかの操作を実行します：
 - スライダーを上下させて、事前に設定されたセキュリティレベルを選択します。
選択できるセキュリティレベルは、次の通りです：
 - **最大の保護**：開いているファイル、保存されているファイル、または実行されているファイルを最大限に監視します。
 - **推奨**：カスペルスキーが推奨する設定に従ってファイルを監視します。
既定ではこのセキュリティレベルが設定されています。
 - **速度重視**：最小限のファイルを監視します。メモリリソースを大量に必要とするアプリケーションを快適に使用したい場合は、このセキュリティレベルを選択してください。
 - セキュリティの設定を手動で編集します：
 - a. [設定] をクリックします。
[設定：スキャン] ウィンドウが表示されます。
 - b. [全般] タブの [ファイル種別] セクションで、スキャンタスクの実行時にスキャンするファイルの種別を選択します。
 - c. [全般] タブの [最適化] セクションで、スキャンパフォーマンスを設定します。
 - d. [全般] タブの [複合ファイル] セクションで、検知するオブジェクトとして分析する複合ファイルを選択します。
 - e. [詳細] タブの [詳細設定] セクションで、iSwift の使用、およびアプリケーションの統計で検知された悪意のあるオブジェクトに関する情報の記録について設定します。
 - f. [詳細] タブの [ヒューリスティックアナライザー] セクションで、ヒューリスティック分析の使用を設定し、マルウェアスキャンの際にヒューリスティック分析によって適用される保護レベルを選択します。
 - g. [OK] をクリックして変更を保存し、[設定：スキャン] ウィンドウを閉じます。
セキュリティレベルが [カスタム] に変更されます。
 - 既定の設定に戻すには、[既定] をクリックします。
セキュリティレベルが [推奨] に変更されます。
4. 必要に応じて、[処理] セクションで、感染したオブジェクトの検知時に実行する処理を選択します。
5. スキャン範囲を指定するには、[スキャン範囲] セクションで [設定] をクリックし、[スキャン範囲] ウィンドウが開いたら次の操作を実行します：
 - a. すべてのリムーバブルドライブをスキャンする場合は、[すべてのリムーバブルディスク] をオンにします。
 - b. すべての内部ドライブをスキャンする場合は、[すべての内部ディスク] をオンにします。
 - c. すべてのネットワークドライブをスキャンする場合は、[すべてのネットワークディスク] をオンにします。
 - d. コンピュータのメモリをスキャンする場合は、[メモリ] をオンにします。
 - e. スタートアップオブジェクトをスキャンする場合は、[ログイン項目] をオンにします。
 - f. 他のファイルやフォルダをスキャンする場合は、[追加] をクリックして、ファイル、フォルダ、またはファイル名やフォルダ名のマスクを指定します。
 - g. [OK] をクリックして変更を保存し、[スキャン範囲] ウィンドウを閉じます。
6. 次のいずれかの方法で、変更を保存します：
 - [適用] をクリックし、**タスクのプロパティ**ウィンドウが開いたままの状態に変更を保存します。

- [OK] をクリックし、変更を保存して**タスクのプロパティ**ウィンドウを閉じます。

アップデートタスクの設定を管理する[?]

1. アップデートタスクの設定ウィンドウを開きます。
2. [アップデート] セクションを選択します。
3. 定義データベースとともにソフトウェアモジュールをアップデートする場合は、[ソフトウェアモジュールをアップデートする] をオンにします。
4. アップデート元を選択するには：
 - a. [設定] をクリックします。
[設定：アップデート] ウィンドウが表示されます。
 - b. 次のいずれかの方法で、アップデート元を指定します：
 - 管理サーバーからアップデートをダウンロードする場合は、[Kaspersky Security Center] をオンにします。
 - カスペルスキーのアップデートサーバからアップデートをダウンロードする場合は、[カスペルスキーのアップデートサーバ] をオンにします。
 - 別のアップデート元を追加するには、[追加] をクリックして、表示されたウィンドウにアップデート元のパスを入力します。
既定では、Kaspersky Endpoint Security はカスペルスキーのアップデートサーバからアップデートをダウンロードします。
 - c. [OK] をクリックして変更を保存し、[設定：アップデート] ウィンドウを閉じます。
5. 次のいずれかの方法で、変更を保存します：
 - [適用] をクリックし、**タスクのプロパティ**ウィンドウが開いたままの状態に変更を保存します。
 - [OK] をクリックし、変更を保存して**タスクのプロパティ**ウィンドウを閉じます。

ローカルタスクのみ

ファイル脅威対策タスクの設定を管理する[?]

1. クライアントコンピュータ向けのローカルタスクのリストを開きます。
2. ローカルタスクのリストで、[ファイル脅威対策] タスクを選択し、次のいずれかの方法でプロパティを開きます：
 - タスク名をダブルクリックします。
 - 右クリックしてタスクのショートカットメニューを表示させ、[プロパティ] を選択します。
 - [プロパティ] をクリックします。
3. [ファイル脅威対策] セクションを選択します。
4. 必要に応じて、次の設定を編集します：
 - クライアントコンピュータ上で、ファイル脅威対策を有効または無効にします。
 - [セキュリティレベル] セクションで、事前に設定されているセキュリティレベルのいずれかをスライダーを使用して選択します。
 - セキュリティ設定を手動で編集するには、[設定] をクリックし、[設定：ファイル脅威対策] ウィンドウが開いたら次を行います：
 - a. [全般] タブの [ファイル種別] セクションで、ファイルに対して開く、実行、または保存の操作の実行時に Kaspersky Endpoint Security がスキャンするファイルの種別を選択します。
 - b. [全般] セクションの [最適化] セクションで、スキャンパフォーマンスとスキャン技術を設定します。また、読み取り専用ボリュームのスキャンをスキップするかどうかを選択します。
 - c. [全般] セクションの [複合ファイル] タブで、検知対象のオブジェクトとしてスキャンする複合ファイルを選択し、サイズの大きいオブジェクトをスキャンする時の制限を設定します。

d. **〔保護範囲〕** タブで、ファイル脅威対策のスキャン対象にするファイルまたはフォルダを指定します。

既定では、クライアントコンピュータに接続されているリムーバブルドライブ、内部ドライブ、およびネットワークドライブにあるすべてのオブジェクトがスキャンされます。保護範囲へのオブジェクトの追加、リスト内のオブジェクトの変更、リスト内のオブジェクトのスキャンの一時無効化、またはリストからのオブジェクトの削除を行うことができます。

e. **〔詳細〕** タブの **〔スキャン方法〕** セクションで、ファイル脅威対策の方法を選択します。

f. **〔詳細〕** タブの **〔タスクの一時停止〕** セクションでは、スケジュールされたファイルアンチウイルスの一時停止の有効化と無効化の切り替えや、スケジュールに従って自動的にタスクを一時停止する設定を指定できます。

g. **〔詳細〕** タブの **〔ヒューリスティックアナライザー〕** セクションでは、ファイル脅威対策でヒューリスティック分析を使用するかどうかを設定できます。

h. **〔OK〕** をクリックして変更を保存し、**〔設定：ファイル脅威対策〕** ウィンドウを閉じます。

- **〔悪意のあるオブジェクトが検知された場合〕** セクションでは、感染したオブジェクトの検知時に、ファイル脅威対策が実行する処理を選択できます。

5. 次のいずれかの方法で、変更を保存します：

- **〔適用〕** をクリックすると、**ファイル脅威対策のプロパティ** ウィンドウが開いたままの状態に変更が保存されます。
- **〔OK〕** をクリックすると、変更が保存されて、**ファイル脅威対策のプロパティ** ウィンドウが閉じます。

ウェブ脅威対策タスクの設定を管理する

1. クライアントコンピュータ向けのローカルタスクのリストを開きます。

2. ローカルタスクのリストで、**〔ウェブ脅威対策〕** タスクを選択し、次のいずれかの方法でプロパティを開きます：

- タスク名をダブルクリックします。
- 右クリックしてタスクのショートカットメニューを表示させ、**〔プロパティ〕** を選択します。
- **〔プロパティ〕** をクリックします。

3. **〔ウェブ脅威対策〕** セクションを選択します。

4. 必要に応じて、次の設定を編集します：

- クライアントコンピュータ上で、ウェブ脅威対策を有効または無効にします。
- **〔セキュリティレベル〕** セクションで、事前に設定されているセキュリティレベルのいずれかをスライダーを使用して選択します。
- セキュリティ設定を手動で編集するには、**〔設定〕** をクリックし、**〔設定：ウェブ脅威対策〕** ウィンドウが開いたら次を行います：
 - a. **〔全般〕** タブの **〔スキャン方法〕** セクションで、URL が悪意のある URL のデータベースに登録されているかどうかを確認するオプションを有効または無効にします。
 - b. **〔全般〕** タブの **〔アンチフィッシング設定〕** セクションで、URL がフィッシングアドレスのデータベースに登録されているかどうかを確認するオプションを有効または無効にします。
 - c. **〔全般〕** タブの **〔アンチフィッシング設定〕** セクションで、フィッシングサイトへのリンクを検知するためのヒューリスティック分析の使用を有効または無効にします。
 - d. **〔信頼する URL〕** タブで、信頼する URL からの Web トラフィックのスキャンを有効または無効にするか、信頼する URL のリストを作成または編集します。
 - e. **〔OK〕** をクリックして変更を保存し、**〔設定：ウェブ脅威対策〕** ウィンドウを閉じます。

5. **〔悪意のあるオブジェクトが検知された場合〕** セクションでは、Web トラフィックでの危険なオブジェクトの検知時に、ウェブアンチウイルスが実行する処理を選択できます。

6. 次のいずれかの方法で、変更を保存します：

- **〔適用〕** をクリックし、**ウェブ脅威対策のプロパティ** ウィンドウが開いたままの状態に変更を保存します。
- **〔OK〕** をクリックして変更を保存し、**ウェブ脅威対策のプロパティ** ウィンドウを閉じます。

簡易スキャンタスクの設定を管理する

1. クライアントコンピュータ向けのローカルタスクのリストを開きます。
2. ローカルタスクのリストで、[簡易スキャン] タスクを選択し、次のいずれかの方法でプロパティを開きます：
 - タスク名をダブルクリックします。
 - 右クリックしてタスクのショートカットメニューを表示させ、[プロパティ] を選択します。
 - [プロパティ] をクリックします。
3. [スキャン] セクションを選択します。
4. 必要に応じて、次の設定を編集します：
 - [セキュリティレベル] セクションで、事前に設定されているセキュリティレベルのいずれかをスライダーを使用して選択します。
 - セキュリティ設定を手動で編集するには、[設定] をクリックし、[設定：スキャン] ウィンドウが開いたら次を行います：
 - a. [全般] タブの [ファイル種別] セクションで、スキャン対象にするファイルの種別を選択します。
 - b. [全般] タブの [最適化] セクションで、スキャンパフォーマンスを設定します。
 - c. [全般] タブの [複合ファイル] セクションで、スキャン対象にする複合ファイルを選択します。
 - d. [詳細] タブの [詳細設定] セクションで、iSwift の使用、およびアプリケーションの統計で検知された悪意のあるオブジェクトに関する情報の記録について設定します。
 - e. [詳細] タブの [ヒューリスティックアナライザー] セクションで、ヒューリスティック分析の使用を設定し、ヒューリスティック分析によって適用される保護レベルを選択します。
 - f. [OK] をクリックして変更を保存し、[設定：スキャン] ウィンドウを閉じます。
 - [処理] セクションでは、感染したオブジェクトの検知時に Kaspersky Endpoint Security が実行する処理を選択できます。
 - スキャン範囲を指定するには、[スキャン範囲] セクションで [設定] をクリックし、[スキャン範囲] ウィンドウが開いたら次の操作を実行します：
 - 既定のリスト内のオブジェクトをスキャンする場合は、対象のオブジェクトに隣接するチェックボックスをオンにします。
 - 他のファイルやフォルダをスキャンする場合は、[追加] をクリックして、ファイル、フォルダ、またはファイル名やフォルダ名のマスクを指定します。
 - [OK] をクリックして変更を保存し、[スキャン範囲] ウィンドウを閉じます。
5. 次のいずれかの方法で、変更を保存します：
 - [適用] をクリックし、簡易スキャンのプロパティウィンドウが開いたままの状態に変更を保存します。
 - [OK] をクリックし変更を保存して、簡易スキャンのプロパティウィンドウを閉じます。

完全スキャンタスクの設定を管理する ②

1. クライアントコンピュータ向けのローカルタスクのリストを開きます。
2. ローカルタスクのリストで、[完全スキャン] タスクを選択し、次のいずれかの方法でプロパティを開きます：
 - タスク名をダブルクリックします。
 - 右クリックしてタスクのショートカットメニューを表示させ、[プロパティ] を選択します。
 - [プロパティ] をクリックします。
3. [スキャン] セクションを選択します。
4. 必要に応じて、次の設定を編集します：
 - [セキュリティレベル] セクションで、事前に設定されているセキュリティレベルのいずれかをスライダーを使用して選択します。
 - セキュリティ設定を手動で編集するには、[設定] をクリックし、[設定：スキャン] ウィンドウが開いたら次を行います：

- a. **[全般]** タブの **[ファイル種別]** セクションで、スキャン対象にするファイルの種別を選択します。
 - b. **[全般]** タブの **[最適化]** セクションで、スキャンパフォーマンスを設定します。
 - c. **[全般]** タブの **[複合ファイル]** セクションで、スキャン対象にする複合ファイルを選択します。
 - d. **[詳細]** タブの **[詳細設定]** セクションで、iSwift の使用、およびアプリケーションの統計で検知された悪意のあるオブジェクトに関する情報の記録について設定します。
 - e. **[詳細]** タブの **[ヒューリスティックアナライザー]** セクションで、ヒューリスティック分析の使用を設定し、ヒューリスティック分析によって適用される保護レベルを選択します。
 - f. **[OK]** をクリックして変更を保存し、**[設定：スキャン]** ウィンドウを閉じます。
- **[処理]** セクションでは、感染したオブジェクトの検知時に Kaspersky Endpoint Security が実行する処理を選択できます。
 - スキャン範囲を指定するには、**[スキャン範囲]** セクションで **[設定]** をクリックし、**[スキャン範囲]** ウィンドウが開いたら次の操作を実行します：
 - 既定のリスト内のオブジェクトをスキャンする場合は、対象のオブジェクトに隣接するチェックボックスをオンにします。
 - 他のファイルやフォルダをスキャンする場合は、**[追加]** をクリックして、ファイル、フォルダ、またはファイル名やフォルダ名のマスクを指定します。
 - **[OK]** をクリックして変更を保存し、**[スキャン範囲]** ウィンドウを閉じます。
5. 次のいずれかの方法で、変更を保存します：
- **[適用]** をクリックし、**完全スキャンのプロパティ** ウィンドウが開いたままの状態に変更を保存します。
 - **[OK]** をクリックし、変更を保存して、**完全スキャンのプロパティ** ウィンドウを閉じます。

オブジェクトスキャンタスクの設定を管理する^⑦

1. クライアントコンピュータ向けのローカルタスクのリストを開きます。
2. ローカルタスクのリストで、**[オブジェクトスキャン]** タスクを選択し、次のいずれかの方法でプロパティを開きます：
 - タスク名をダブルクリックします。
 - 右クリックしてタスクのショートカットメニューを表示させ、**[プロパティ]** を選択します。
 - **[プロパティ]** をクリックします。
3. **[スキャン]** セクションを選択します。
4. 必要に応じて、次の設定を編集します：
 - **[セキュリティレベル]** セクションで、事前に設定されているセキュリティレベルのいずれかをスライダーを使用して選択します。
 - セキュリティ設定を手動で編集するには、**[設定]** をクリックし、**[設定：スキャン]** ウィンドウが開いたら次を行います：
 - a. **[全般]** タブの **[ファイル種別]** セクションで、スキャン対象にするファイルの種別を選択します。
 - b. **[全般]** タブの **[最適化]** セクションで、スキャンパフォーマンスを設定します。
 - c. **[全般]** タブの **[複合ファイル]** セクションで、スキャン対象にする複合ファイルを選択します。
 - d. **[詳細]** タブの **[詳細設定]** セクションで、iSwift の使用、およびアプリケーションの統計で検知された悪意のあるオブジェクトに関する情報の記録について設定します。
 - e. **[詳細]** タブの **[ヒューリスティックアナライザー]** セクションで、ヒューリスティック分析の使用を設定し、ヒューリスティック分析によって適用される保護レベルを選択します。
 - f. **[OK]** をクリックして変更を保存し、**[設定：スキャン]** ウィンドウを閉じます。
 - **[処理]** セクションでは、感染したオブジェクトの検知時に Kaspersky Endpoint Security が実行する処理を選択できます。
 - スキャン範囲を指定するには、**[スキャン範囲]** セクションで **[設定]** をクリックし、**[スキャン範囲]** ウィンドウが開いたら次の操作を実行します：

- **[追加]** をクリックして、ファイル、フォルダ、またはファイル名やフォルダ名のマスクを指定します。
- **[OK]** をクリックして変更を保存し、**[スキャン範囲]** ウィンドウを閉じます。

5. 次のいずれかの方法で、変更を保存します：

- **[適用]** をクリックし、**オブジェクトスキャンのプロパティ** ウィンドウを開いたままの状態に変更を保存します。
- **[OK]** をクリックし変更を保存して、**オブジェクトスキャンのプロパティ** ウィンドウを閉じます。

ネットワーク脅威対策タスクの設定を管理する^⑦

1. クライアントコンピュータ向けのローカルタスクのリストを開きます。
2. ローカルタスクのリストで、**[ネットワーク脅威対策]** タスクを選択し、次のいずれかの方法でプロパティを開きます：
 - タスク名をダブルクリックします。
 - 右クリックしてタスクのショートカットメニューを表示させ、**[プロパティ]** を選択します。
 - **[プロパティ]** をクリックします。
3. **[ネットワーク脅威対策]** セクションを選択します。
4. 必要に応じて、次の設定を編集します：
 - クライアントコンピュータ上で、ネットワーク脅威対策を有効または無効にします。
 - **[ネットワーク脅威対策の設定]** セクションの **[攻撃を行っているコンピュータをブロックする時間]** をオンまたはオフにし、値を指定します。
 - ネットワーク活動をブロックしないコンピュータの IP アドレスを指定することもできます。それには、次の操作を実行します：
 - a. **[除外リスト]** をクリックします。
[除外] ウィンドウが表示されます。
 - b. **[追加]** をクリックします。
[IP アドレス] ウィンドウが表示されます。
 - c. ネットワーク活動をブロックしないコンピュータの IP アドレスを指定し、**[OK]** をクリックします。
 - d. **[OK]** をクリックして変更を保存し、**[除外]** ウィンドウを閉じます。
5. 次のいずれかの方法で、変更を保存します：
 - **[適用]** をクリックし、**ネットワーク脅威対策のプロパティ** ウィンドウが開いたままの状態に変更を保存します。
 - **[OK]** をクリックして変更を保存し、**ネットワーク脅威対策のプロパティ** ウィンドウを閉じます。

ポリシーの作成と管理

このセクションでは、Kaspersky Endpoint Security のポリシーの作成と設定方法について説明します。

ポリシーは、アプリケーションの設定を決定するとともに、管理グループ内のコンピュータにインストールされたアプリケーションの設定へのアクセスを管理します。各アプリケーションについて個別にポリシーを作成する必要があります。各管理グループのコンピュータにインストールされたアプリケーション向けに複数のポリシーを作成できますが、各管理グループ内で1つのアプリケーションについて一度に適用されるポリシーは1つのみです。

注意：ポリシーの作成や設定を行う場合、 および  を使用して、ポリシー内の任意の設定のグループに対する変更を禁止または許可できます。

カスタムポリシーでは、次の操作を実行できます：

- ポリシーの作成
- ポリシーの設定
- あるグループから別のグループへのポリシーのコピーおよび移動

- ポリシーの削除
- ポリシーのステータスの変更
- ファイルへのポリシーのエクスポート
- ファイルからのポリシーのインポート

Kaspersky Security Center のポリシーの詳細は、[Kaspersky Security Center のヘルプ](#) を参照してください。

ポリシーの作成

このセクションでは、新規ポリシーウィザードを起動してポリシーを作成する方法について説明します。

[管理グループのフォルダからポリシーを作成する](#)

1. Kaspersky Security Center の管理コンソールを起動します。
2. [管理サーバ - <サーバ名>] フォルダを展開します。
3. コンソールツリーで、[管理対象デバイス] をクリックします。
4. 対象のクライアントコンピュータが含まれた管理グループを選択します。
5. 作業領域で、[ポリシー] タブを選択し、[新規ポリシー] をクリックします。
新規ポリシーウィザードが開きます。
6. 新規ポリシーウィザードの手順に従って、ポリシーを作成します。

[「ポリシー」フォルダからポリシーを作成する](#)

1. Kaspersky Security Center の管理コンソールを起動します。
2. [管理サーバ - <サーバ名>] フォルダを展開します。
3. コンソールツリーで、[ポリシー] をクリックします。
4. 作業領域で、[新規ポリシー] をクリックします。
新規ポリシーウィザードが開きます。
5. 新規ポリシーウィザードの手順に従って、ポリシーを作成します。

ウィザードの次の手順に進むには、[次へ] をクリックします。ウィザードの前の手順に戻るには、← をクリックします。ウィザードを途中で停止するには、[キャンセル] をクリックします。

注意： ボタンの外観は、Windows のバージョンによって異なる場合があります。

[ステップ 1: アプリケーションの選択](#)

[グループポリシー作成対象のアプリケーションを選択] ウィンドウで、アプリケーションのリストから [Kaspersky Endpoint Security for Mac (12.2)] を選択します。

[ステップ 2: ポリシー名の指定](#)

1. [グループポリシーの名前を入力] ウィンドウの [名前] に、作成するポリシーの名前を指定します。次の記号は使用できません： “ * < : > ? \ | 。
2. Kaspersky Endpoint Security の既存のポリシーから新しいポリシーに設定をインポートする場合は、[旧バージョンのアプリケーションのポリシーの設定を使用する] をオンにします。

[ステップ 3: プロテクション設定の指定](#)

[**プロテクション**] ウィンドウで、必要に応じて次の設定を指定します：

- クライアントコンピュータのオペレーティングシステムの保護を設定します。
- 信頼ゾーンを設定します。
Kaspersky Endpoint Security でスキャンや監視の対象外となる、オブジェクトのリストを作成することができます。
- 信頼済みアプリケーションを設定します。
Kaspersky Endpoint Security でネットワーク活動とファイル操作が監視の対象外となるアプリケーションのリストを作成できます。
- 検知するオブジェクトの種別を選択します。
- コンピュータがバッテリーで稼働している時、スケジュールされたタスクの起動を有効または無効にします。
- スキャンタスクによる CPU の使用を制限します。

ステップ4：ファイル脅威対策の設定

[**ファイル脅威対策**] ウィンドウで、必要に応じて次を設定します：

- ファイル脅威対策を有効または無効にします。
既定では、ファイル脅威対策は有効になっています。
- セキュリティレベルを選択する。
既定では、カスペルスキーが推奨するセキュリティレベルが選択されています。
- ファイル脅威対策を設定します。
- 悪意のあるオブジェクトの検知時に実行する処理を選択します。

ステップ5：ウェブ脅威対策の設定

[**ウェブ脅威対策**] ウィンドウで、必要に応じて次の設定を行います：

- ウェブ脅威対策を有効または無効にします。
既定では、ウェブ脅威対策は有効になっています。
- セキュリティレベルを選択する。
既定では、カスペルスキーが推奨するセキュリティレベルが選択されています。
- ウェブ脅威対策の設定。
- Web トラフィックで悪意のあるオブジェクトを検知した時に実行する処理を選択します。

ステップ6：ネットワーク脅威対策の設定

[**ネットワーク脅威対策**] ウィンドウで、必要に応じて次の設定を行います：

- ネットワーク脅威対策を有効または無効にします。
既定では、ネットワーク脅威対策が有効になっています。
- ネットワーク脅威対策の設定を編集します。
- ネットワーク活動が Kaspersky Endpoint Security によってブロックされないリモートコンピュータの IP アドレスのリストを作成または編集します。

ステップ7：アップデートの設定

[**アップデート**] ウィンドウで、必要に応じて次を行います：

- ソフトウェアモジュールのアップデートを有効または無効にする。
- アップデート元を指定します。

[Kaspersky Security Network] ウィンドウで、必要に応じて次の設定を行います：

- [KSN 声明] をクリックして、Kaspersky Security Network 声明のテキスト全文を読む。
- Kaspersky Security Center から提供される KSN インフラストラクチャに関する情報を表示します。
- Kaspersky Security Network の使用を有効または無効にします。
- 拡張 KSN モードを有効または無効にします。
- KSN プロキシの使用を有効または無効にします。
- KSN プロキシが使用できない場合、カスペルスキーのサーバの使用を有効または無効にします。

注意：Kaspersky Security Network と KSN プロキシをリモートコンピュータで使用可能なのは、Kaspersky Security Center 管理サーバーがプロキシサーバとして使用されている場合のみです。管理サーバーのプロパティの詳細は、[Kaspersky Security Center のヘルプ](#)を参照してください。

ポリシーの設定で、Kaspersky Security Center によってグローバル KSN インフラストラクチャが使用されており、かつ、Kaspersky Security Network への参加を選択すると、ポリシーが適用されたクライアントコンピュータにおける Kaspersky Endpoint Security の統計情報が自動的にカスペルスキーに送信され、それらのコンピュータをより強力に保護できるようになります。

注意：カスペルスキーでは、お客様の明確な同意がない限り、いかなる個人情報の受信、処理、保管も行いません。

グローバル KSN インフラストラクチャの Kaspersky Security Network の使用時にカスペルスキーに提供されるデータ

[Kaspersky Security Network の使用に同意する] をオンにし、[拡張 KSN モードを有効にする] をオフにすると、次のデータがカスペルスキーに提供されます：

- 適用されているライセンスの情報：ライセンスの種別および有効期間、ライセンスの有効期限までの日数、ライセンスの購入元である代理店の識別子、地域のアクティベーションセンターの識別子、アクティベーションコードのチェックサム、SHA1 アルゴリズムを使用して計算されたチケットボディのハッシュ、ライセンスチケットの作成日時、ライセンス情報の識別子、ライセンスチケットの識別子、ライセンスチケットのシーケンスの識別子、ユーザのコンピュータの一意な識別子、ライセンスチケットが有効になった日付、ライセンスチケットの有効期限、ライセンスチケットの現在のステータス、チケットヘッダーのバージョン、ライセンスのバージョン、チケットヘッダーの署名に使用された証明書の識別子、ライセンスファイルのチェックサム、チケットヘッダーの署名元のシリアル番号、認証トークン。
- インストールされた本ソフトウェアの詳細バージョン。

インストールされた本ソフトウェアの種別。ソフトウェアアップデートの ID。評価サービスの ID。プロトコルタイプの ID。地域のアクティベーションセンターの ID。本ソフトウェアのサービスの決定のうち取り消されたもののリストのバージョン。トリガーされた本ソフトウェアの定義データベースのレコードの ID。トリガーされた本ソフトウェアの定義データベースのレコードのタイムスタンプ。トリガーされた本ソフトウェアの定義データベースのレコードの種別。本ソフトウェアのコンピュータへのインストールのインスタンスの一意な ID。ライセンスがアクティベートされた日付。ライセンスの有効期限日。ライセンスの識別子。本ソフトウェアが使用中のライセンスのステータス。処理中のオブジェクトのチェックサム種別。検知されたマルウェアの名前、ユーザのコンピュータまたはデータに損害を与える目的で使用される可能性がある正規のソフトウェアの名前。処理中のオブジェクトのチェックサム。本ソフトウェアのアクティベーションコードのチェックサム。本ソフトウェアの詳細バージョン。一意のデバイス ID。本ソフトウェアの ID。本ソフトウェアのライセンス情報ファイルのチェックサム。本ソフトウェアのライセンスの提供に使用された情報形式の ID。本ソフトウェアのライセンスチケットのヘッダーへの署名に使用される証明書の識別子。本ソフトウェアのライセンスチケットの作成日時。本ソフトウェアのライセンスチケットのチェックサム。本ソフトウェアのライセンスチケットのバージョン。本ソフトウェアのアクティベーションコードのバージョン。権利者のインフラストラクチャへのリクエストに含まれるデータの形式。使用中のライセンスチケットの ID。本ソフトウェアのコンポーネントの ID。本ソフトウェアの動作の結果。エラーコード。アクセスされた Web サービスのアドレス (URL、IP)。ポート番号。Web サービスのリクエスト元の URL (リファラー)。証明書の公開鍵。スキャンされたオブジェクトのデジタル証明書のサムプリントとハッシュアルゴリズム。

[Kaspersky Security Network の使用に同意する] と [拡張 KSN モードを有効にする] をオンにすると、次のデータがカスペルスキーに提供されます：

- コンピュータにインストールされているオペレーティングシステム (OS) やサービスパックのバージョンに関する情報、OS カーネルファイルのバージョンおよびチェックサム (MD5、SHA2-256、SHA1)、OS 実行モードの識別子。OS のバージョン、OS のビルド番号、OS のアップデート番号、OS のエディション、OS のエディションに関する詳細情報。OS のサービスパックのバージョン OS の起動日時。ふるまい分析のサブシステムにおける OS 動作に関するイベントの処理遅延時間。現在の種別の遅延された OS 動作イベントの数。プロアクティブディフェンスのサブシステムにおける OS 動作に関するイベントの処理遅延時間。処理された OS 動作イベントの数。処理された OS 同期動作イベントの数。現在の種別のすべての OS 動作イベントの合計遅延時間。持続的イベントを記憶するサブシステムにおける、OS 動作に関するイベントの処理遅延時間。すべての OS 動作イベントの合計遅延。待機中の OS 同期動作イベントの数。OS 内の動作イベントを受信した日時。

- 以前、OSの再起動が失敗した履歴：再起動に失敗した回数。
- インストールされている本製品に関する情報およびアンチウイルス保護状況：ソフトウェアのインストール識別子（PCID）本ソフトウェアの定義データベースのレコードのバージョン、コンピュータ上にインストールされたアプリケーションのインスタンスの一意な識別子、アプリケーションの種別、アプリケーション種別の識別子、インストールされたアプリケーションの詳細バージョン、アプリケーションの設定のバージョンの識別子、コンピュータ種別の識別子、アプリケーションがインストールされたコンピュータの一意な識別子、権利者のサービスにおける一意なユーザー識別子、言語および動作状況、インストールされたソフトウェアコンポーネントのバージョンと動作状況、権利者のサービスに接続するために使用されたプロトコルのバージョン、インストールされた本ソフトウェアの詳細バージョン。インストールされた本ソフトウェアの種別。ソフトウェアアップデートのID。評価サービスのID。プロトコルタイプのID。地域のアクティベーションセンターのID。本ソフトウェアのサービスの決定のうち取り消されたもののリストのバージョン。トリガーされた本ソフトウェアの定義データベースのレコードのID。トリガーされた本ソフトウェアの定義データベースのレコードのタイムスタンプ。トリガーされた本ソフトウェアの定義データベースのレコードの種別。本ソフトウェアのコンピュータへのインストールのインスタンスの一意なID。ライセンスがアクティベートされた日付。ライセンスの有効期限日。ライセンスの識別子。本ソフトウェアが使用中のライセンスのステータス。処理中のオブジェクトのチェックサム種別。検知されたマルウェアの名前、ユーザのコンピュータまたはデータに損害を与える目的で使用される可能性がある正規のソフトウェアの名前。処理中のオブジェクトのチェックサム。本ソフトウェアのアクティベーションコードのチェックサム。本ソフトウェアの詳細バージョン。本ソフトウェアのID。本ソフトウェアのライセンス情報ファイルのチェックサム。本ソフトウェアのライセンスの提供に使用された情報形式のID。本ソフトウェアのライセンスチケットのヘッダーへの署名に使用される証明書の識別子。本ソフトウェアのライセンスチケットの作成日時。本ソフトウェアのライセンスチケットのチェックサム。本ソフトウェアのライセンスチケットのバージョン。本ソフトウェアのアクティベーションコードのバージョン。権利者のインフラストラクチャへのリクエストに含まれるデータの形式。使用中のライセンスチケットのID。本ソフトウェアのコンポーネントのID。本ソフトウェアの動作の結果。エラーコード。アクセスされたWebサービスのアドレス（URL、IP）。ポート番号。Webサービスのリクエスト元のURL（リファラー）。定義データベースのアップデートと適用のサイクル数。定義データベースが最後にアップデートおよび適用された日時。本ソフトウェアの定義データベースの公開日時。本ソフトウェアのコンポーネントのバージョン。ソフトウェアアップデートのID。インストールされた本ソフトウェアの種別。システムウォッチャーの開始日時。本ソフトウェアのインストール日時。システムウォッチャーによって統計が送信される確率。システムウォッチャーによる標準処理時間よりも長い時間がかかったイベントのコード。システムウォッチャーによる標準処理時間を超えたイベントのデータベース処理時間。システムウォッチャーによるイベントの処理に許可される最大時間。システムウォッチャーによる標準処理時間を超えたイベントの処理時間。システムウォッチャーによる標準処理時間よりも長い時間がかかったイベントの総数。
- 処理したすべてのオブジェクトおよび操作に関する情報：処理中のオブジェクトに対する本ソフトウェアの判定、ディレクトリコード、処理中のオブジェクトのサイズ、処理中のオブジェクトのチェックサム（SHA256）、システムウォッチャーを使用して検知されたソフトウェアの数、システムウォッチャーでソフトウェアを検知した日時、検知の特性、トリガーされた本ソフトウェアの定義データベースのレコードのID。システムウォッチャーでソフトウェアを検知した理由、処理中のオブジェクトのチェックサム（MD5）、モジュールの整合性チェックの結果、処理中のオブジェクトの名前、トリガーされた本ソフトウェアの定義データベースのレコードの種別、処理中のオブジェクトへのパス。スキャンしたオブジェクトの製造元の名前、スキャンの日時、URLおよびダウンロードされたリファラーのアドレス、スキャンされたファイルのサイズおよびパス、アーカイブかどうかのフラグ、ファイルの作成日時、圧縮されていた場合はパッカーの名前、サイズおよびチェックサム（MD5、SHA2-256）、ファイルのエントロピー、ファイルの種別、ファイル種別コード、ファイルが実行可能であるかどうかのフラグ、識別子および形式、オブジェクトのチェックサム（MD5、SHA2-256）、オブジェクトの追加チェックサムの種別および値、オブジェクトのデジタル署名（証明書）に関するデータ：証明書の発行元に関する情報、前回の統計が送信されてからオブジェクトが実行された回数、本製品のスキータスクの識別子、オブジェクトの評価に関する情報の受信手段、TARGET フィルターの値、適用可能な検知技術の技術的パラメータ。処理中のオブジェクトへのパス。ディレクトリコード。
- 実行ファイルの場合：ファイルセクションの情報量、評価の検証フラグまたはファイルの署名フラグ、検証対象のオブジェクトに読み込まれたアプリケーションの名前、種別、ID 種別、チェックサム（MD5）およびサイズ、アプリケーションのパスおよびテンプレートのパス、自動実行リストの署名、エントリの日時、属性のリスト、圧縮ソフトウェアの名前、アプリケーションのデジタル署名に関する情報：発行者の証明書、アップロードされたファイルのMIME形式での名前、ファイルが作成された日時。
- 実行中のアプリケーションおよびそのモジュールに関する情報：実行中のファイルのチェックサム（MD5、SHA2-256）、ファイルのサイズ、属性、作成日時、圧縮ソフトウェアの名前（ファイルが圧縮されている場合）、ファイル名、システム上で実行されているプロセスに関する情報（プロセスID（PID）、プロセス名、プロセスを開始したアカウントに関する情報、プロセスを開始したアプリケーションおよびコマンド、プロセスのファイルへの完全パスおよび開始したコマンドライン、プロセスが属するアプリケーションの説明（アプリケーション名および配信元の情報）、使用されるデジタル証明書およびそれらの正当性を検証するために必要な情報またはファイルのデジタル署名が存在しない旨のフラグ）、プロセスに読み込まれたモジュールの情報：名前、サイズ、種別、作成日、属性、チェックサム（MD5、SHA2-256、SHA1）およびパス、PEファイルのヘッダー情報、圧縮ソフトウェア名（ファイルが圧縮されている場合）、統計情報の有効性および使用可否に関する情報、送信される統計情報の生成条件の識別子。
- 脅威または脆弱性が検知された場合、検知されたオブジェクトに関する情報に加え、次の情報が提供されます：定義データベース中のレコードの識別子、バージョンおよび種別、カスペルスキーの分類による脅威名、定義データベースの最終アップデート日時、実行ファイルの名前、脅威が検知されたURLをリクエストしたアプリケーションのファイルのチェックサム（MD5）、検知した脅威のIPアドレス（IPv4またはIPv6）、脆弱性の識別子および脅威レベル、脅威を検知したWebページのURLおよびリファラー。
- 悪意のある可能性があるオブジェクトが検知された場合、プロセスのメモリ内のデータに関する情報が提供されます。
- ネットワーク攻撃の情報：攻撃元コンピュータのIPアドレスおよびユーザのコンピュータ上でネットワーク攻撃の標的にされたポート番号、攻撃プロトコルのID、名前および攻撃種別。
- ネットワーク接続に関する情報：ポートを開いたプロセスを起動したファイルのバージョンおよびチェックサム（MD5、SHA2-256、SHA1）、プロセスのファイルのパスおよびデジタル署名、ローカルおよびリモートのIPアドレス、ローカルおよびリモート接続のポート番号、接続状況、ポートが開かれた時刻。
- 危険なオブジェクトまたは疑わしいオブジェクトを検知したWebページのURLおよびIPアドレス、このURLをリクエストしたファイルの名前、サイズおよびチェックサム、識別子、検知結果の決定基準に使用されたルールの重み係数および度数、攻撃の目的に関する情報。

- インストール済み本ソフトウェアおよび定義データベースのアップデートに関する情報：アップデートタスクの完了状況、アップデート中に発生した可能性のあるエラーの種別、失敗したアップデートの数、アップデートを実行した本ソフトウェア機能の識別子。
- **Kaspersky Security Network (KSN)** の使用に関する情報：KSN の識別子、本ソフトウェアの識別子、本ソフトウェアの詳細バージョン、個人を特定できないようにしたお客様のデバイスの IP アドレス、KSN へのリクエストの実行品質を示す指数、KSN 用パケットの処理品質を示す指数、KSN へのリクエストの件数およびリクエストの種別に関する情報、統計情報の送信を開始した日時と終了した日時、KSN 設定のアップデートに関する情報：アクティブな設定の識別子、受信した設定の識別子、設定のアップデートのエラーコード。
- イベントに関するシステムログ内の情報：イベントのタイムスタンプ、イベントが検知されたログの名前、イベントの種別およびカテゴリ、イベントの発生源の名前およびイベントの説明。
- ファイルおよび URL の評価決定に関する情報：評価が要求された URL とその参照元、接続のプロトコルタイプ、アプリケーション種別の内部識別子、使用されているポートの番号、ユーザ識別子、スキャンされたファイルのチェックサム (MD5)、検知された脅威の種別、脅威の検知に使用したレコードに関する情報 (定義データベースのレコードの識別子、レコードのタイムスタンプと種別)。証明書の公開鍵。スキャンされたオブジェクトのデジタル証明書のサムプリントとハッシュアルゴリズム。
- 本ソフトウェアの地域分布に関する情報：本ソフトウェアのインストールおよびアクティベーションの日時、本ソフトウェアのアクティベーション用のライセンスを提供した代理店の識別子、本ソフトウェアの識別子、本ソフトウェアの言語版の識別子、本ソフトウェアに適用されたライセンスの識別番号、KSN に参加しているかどうかのフラグ。
- 適用されているライセンスの情報：ライセンスの種別および有効期間、ライセンスの有効期限までの日数、ライセンスの購入元である代理店の識別子、地域のアクティベーションセンターの識別子、アクティベーションコードのチェックサム、SHA1 アルゴリズムを使用して計算されたチケットボディのハッシュ、ライセンスチケットの作成日時、ライセンス情報の識別子、ライセンスチケットの識別子、ライセンスチケットのシーケンスの識別子、ユーザのコンピュータの一意的識別子、ライセンスチケットが有効になった日付、ライセンスチケットの有効期限、ライセンスチケットの現在のステータス、チケットヘッダーのバージョン、ライセンスのバージョン、チケットヘッダーの署名に使用された証明書の識別子、ライセンスファイルのチェックサム、チケットヘッダーの署名元のシリアル番号、認証トークン。
- コンピュータにインストールされているハードウェアに関する情報：搭載または接続された装置の種別、名前、機種名、ファームウェアのバージョン、パラメータ。
- 端末に関する情報：端末の識別子。
- ウェブコントロール機能の動作に関する情報：

機能のバージョン、当該カテゴリに分類された理由および関連情報、分類された URL、ブロックまたは分類されたオブジェクトのホストの IP アドレス。

ポリシーの設定で、**Kaspersky Security Center** によってプライベート KSN インフラストラクチャが使用されており、かつ、**Kaspersky Security Network** への参加を選択すると、**Kaspersky Endpoint Security** は、ポリシーが適用されたクライアントコンピュータからの統計情報をカスペルスキーに送信しなくなります。

ポリシーが削除されたり、非アクティブに変更されたりした後、クライアントの KSN 設定は元の状態に戻ります。

ステップ 9：ユーザインターフェイスの設定

必要に応じて、**[ユーザインターフェイス]** ウィンドウで、**Kaspersky Endpoint Security** とクライアントコンピュータのユーザとの対話インターフェイスを設定できます。

ステップ 10：ネットワーク接続の設定

[ネットワーク] ウィンドウで、必要に応じて次を行います：

- プロキシサーバへの接続を設定します。
- 送受信する HTTPS トラフィックのスキャンを有効または無効にします。
- **Mozilla Firefox** ブラウザで暗号化された HTTPS トラフィックをチェックするための証明書ストアを選択します。
- 信頼済みルート証明書のリストを管理します。
- 監視対象ポートを設定します。
Kaspersky Endpoint Security で監視するポートのリストを作成します。

ステップ 11：レポートとバックアップの設定

[レポートとバックアップ] ウィンドウで、必要に応じて次の設定を行います：

- レポートの生成および保存を設定します。
- バックアップへのオブジェクトの保存を設定します。

ステップ 12：FileVault ディスク暗号化の設定

[FileVault ディスク暗号化] ウィンドウで、必要に応じて次の設定を行います：

- ユーザの起動ディスク向けの FileVault ディスク暗号化の管理を有効または無効にします。
既定では、FileVault ディスク暗号化の管理は無効になっています。
- クライアントコンピュータにポリシーが適用された時にユーザの起動ディスクを暗号化するには、[ディスクを暗号化する] を選択します。

[FileVault ディスク暗号化の管理を有効にする] をオフにすると、管理者権限のあるユーザはシステム設定から Mac の起動ディスクを暗号化および復号化できます。

[FileVault ディスク暗号化の管理を有効にする] と [ディスクを暗号化する] をオンにすると、管理者権限のあるユーザがシステム設定から Mac の起動ディスクを復号化することはできません。

[FileVault ディスク暗号化の管理を有効にする] と [ディスクを復号化する] をオンにすると、管理者権限のあるユーザがシステム設定から Mac の起動ディスクを暗号化することはできません。

ステップ 13：ウェブコントロールの設定

[ウェブコントロール] ウィンドウで、必要に応じて次の設定を行います：

- ウェブコントロールを有効または無効にします。

注意： ウェブコントロールを有効にして危険な Web サイトをブロックすると、[ウェブコントロールが有効です] という通知がリモートコンピュータのプロテクションセンターに表示されます。
新規ポリシーウィザードのウィンドウの [ネットワーク] セクションで [セキュアな接続 (HTTPS) をチェック] をオンにすると、リモートコンピュータ上でウェブコントロールがブロックする Web サイトにユーザがアクセスすると通知が表示されます。

- ウェブコントロールに新しいルールを追加するには、[追加] をクリックします。
ルール名を入力したり、ルールをアクティブにするかどうかを選択したり、特定の URL または Web サイトのカテゴリのリストを作成してルールの適用範囲を指定したり、ルールに含まれる Web サイトへユーザがアクセスした時の処理を選択したりすることができます。
- リスト内に作成したルールを編集、削除、整理します。
ルールの並び順に従って、Kaspersky Endpoint Security が判断する適用の優先順位が決定されます。

ステップ 14：Managed Detection and Response の設定

[Managed Detection and Response] ウィンドウで、必要に応じて次を実行します：

- Managed Detection and Response を有効または無効にします。
既定では、Managed Detection and Response は無効になっています。
- 管理対象デバイスで Managed Detection and Response の有効化に使用する設定情報ファイルをインポートまたは削除します。

[Managed Detection and Response] をオンにして MDR 設定情報ファイルをインポートすると、このコンポーネントがアクティブになり、Kaspersky Managed Detection and Response サービスと対話します。このサービスは、組織を標的とするセキュリティ上の脅威を継続的に検知し、排除します。

ステップ 15：Endpoint Detection and Response (KATA) の設定

[Endpoint Detection and Response (KATA)] ウィンドウで、必要に応じて次の操作を実行します：

- Endpoint Detection and Response (KATA) を有効または無効にします。

既定では、Endpoint Detection and Response (KATA) は無効になっています。

- サーバー接続の設定を指定し、TLS 証明書を追加します。
- KATA サーバーを追加します。

[Endpoint Detection and Response (KATA)] がオンで、TLS 証明書と KATA サーバーが追加されている場合、Endpoint Detection and Response (KATA) コンポーネントが有効になり、Kaspersky Anti Targeted Attack Platform ソリューションと対話します。このソリューションは、標的型攻撃、高度な持続的脅威、ゼロデイ攻撃などの高度な脅威を迅速に検知します。

ステップ 16：外部ディスクのスキャンを設定する

[外部ディスクのスキャン] ウィンドウで、次の設定を指定します：

- 外部ディスクの接続時に Kaspersky Endpoint Security が実行する動作。
- 悪意のあるオブジェクトの検知時に Kaspersky Endpoint Security が実行する処理を指定します。

ステップ 17：ふるまい検知を設定する

[ふるまい検知] ウィンドウで、必要に応じて次の設定を行います：

- ふるまい検知を有効または無効にします。
既定では、ふるまい検知は有効になっています。
- マルウェア活動の検知時に実行する処理を選択します。
- 外部からの暗号化に対する共有フォルダーの保護を有効または無効にします。
 - マルウェア活動の検知時に実行する処理を選択します。

ステップ 18：メール脅威対策を設定する

[メール脅威対策] ウィンドウで、必要に応じて次の設定を行います：

- メール脅威対策を有効または無効にします。
既定では、メール脅威対策が有効になっています。
- 悪意のあるオブジェクトの検知時に実行する処理を選択します。
- メール脅威対策を設定します。

ステップ 19：脆弱性攻撃ブロックを設定する

[脆弱性攻撃ブロック] ウィンドウで、必要に応じて次の設定を行います：

- 脆弱性攻撃ブロックを有効または無効にします。
既定では、脆弱性攻撃ブロックは有効になっています。
- 脆弱性攻撃の検知時に実行する処理を選択します。

ステップ 20：修復エンジンを設定する

[修復エンジン] ウィンドウで、必要に応じて次の設定を行います：

- 修復エンジンを有効または無効にします。
既定では、修復エンジンは有効になっています。

ステップ 21：デバイスコントロールを設定する

[デバイスコントロール] ウィンドウで、必要に応じて次の設定を行います：

- デバイスコントロールを有効または無効にします。
既定では、デバイスコントロールは有効になっています。
- デバイスコントロールを設定します。

ステップ 22：ファイアウォールを設定する

[ファイアウォール] ウィンドウで、必要に応じて次の設定を行います：

- ファイアウォールを有効または無効にします。
既定では、ファイアウォールは有効になっています。
- ファイアウォールを設定します。

ステップ 23：ポリシーを適用する管理グループの定義

[対象グループ] ウィンドウで、[参照] をクリックし、ポリシーを適用する管理グループを選択します。

ステップ 24：ポリシーのステータスの選択とポリシーの作成完了

[アプリケーションのグループポリシーを作成] ウィンドウで、次の操作を実行します：

1. ポリシーに割り当てるステータスを選択します：

- アクティブポリシー - 選択された管理グループにポリシーが適用されます。
- 非アクティブポリシー - ポリシーは適用されません。
- モバイルユーザポリシー - 選択された管理グループが企業ネットワークから接続解除した時にポリシーが適用されます。

注意：管理グループ内の1つのアプリケーションに対して複数のポリシーを作成することができますが、アクティブにできるのは1つのみです。

ポリシーのステータスの詳細は、[Kaspersky Security Center のヘルプ !\[\]\(c183f7dc9b7a352cf91800d107c30d6a_img.jpg\)](#) を参照してください。

2. ポリシーの作成後ポリシーの設定を確認するには、[ポリシーの作成後すぐにプロパティを開く] をオンにします。

3. [終了] をクリックして、新規ポリシーウィザードを終了します。

作成されたポリシーが、関連する管理グループの作業領域にある [ポリシー] タブに表示されます。ポリシーがクライアントコンピュータに適用されるのは、クライアントコンピュータと管理サーバーとの初回の同期後になります。

作成したポリシーの設定を編集できます。設定の各グループにある  および  を使用して、クライアントコンピュータから、グループごとの設定に対する変更を禁止または許可できます。設定のグループに隣接する  は、クライアントコンピュータのユーザが、ユーザのコンピュータ上でこれらの設定を編集できないことを示しています。設定のグループに隣接する  は、クライアントコンピュータのユーザが、ユーザのコンピュータ上でこれらの設定を編集できることを示しています。

ポリシーのリストを表示する

各管理グループのコンピュータにインストールされたアプリケーションについて作成できるポリシーの数に制限はありませんが、各管理グループ内で1つのアプリケーションについて一度に適用されるポリシーは1つだけです。

管理グループのポリシーのリストを表示する

1. Kaspersky Security Center の管理コンソールを起動します。
2. [管理サーバー - <サーバ名>] フォルダを展開します。
3. コンソールツリーで、[管理対象デバイス] をクリックします。

4. 対象のクライアントコンピュータが含まれた管理グループを選択します。

5. 作業領域で、[ポリシー] タブを選択します。
ポリシーのリストが表示されます。

ポリシーの設定

[すべて表示](#) | [すべて隠す](#)

Kaspersky Security Center で作成したポリシーを変更できます。また、サブグループのポリシーとタスクの設定で、ポリシーの設定の変更をブロックできます。

Kaspersky Endpoint Security のポリシーの設定には、アプリケーションの設定と [タスクの設定](#) が含まれます。

ポリシーの設定

1. Kaspersky Security Center の管理コンソールを起動します。
2. [管理サーバ-<サーバ名>] フォルダを展開します。
3. コンソールツリーで、[管理対象デバイス] をクリックします。
4. 作業領域で、[ポリシー] タブを選択します。
5. 設定するポリシーを右クリックして [プロパティ] を選択します。
6. ポリシーのプロパティウィンドウで、ポリシーの設定を編集します：

- [脅威対策] セクション

[ファイル脅威対策の次の設定を編集します：?](#)

- ファイル脅威対策を有効または無効にします。
- 事前に設定されたセキュリティレベルのいずれかを選択するか、セキュリティの設定を手動で編集します。
- 悪意のあるオブジェクトの検知時に実行する処理を選択します。

[ウェブ脅威対策の次の設定を編集します：?](#)

- ウェブ脅威対策を有効または無効にします。
- 事前に設定されたセキュリティレベルのいずれかを選択するか、セキュリティの設定を手動で編集します。
- URL が悪意のある URL のデータベースに登録されているかを確認するかどうかを選択します。
- アンチフィッシングの設定を編集します。
- 信頼する URL を追加します（ウェブ脅威対策でトラフィックがスキャンされなくなります）。
- Web トラフィックで悪意のあるオブジェクトを検知した時に実行する処理を選択します。

[メール脅威対策の次の設定を編集します？](#)

- メール脅威対策を有効または無効にします。
- 悪意のあるオブジェクトの検知時に実行する処理を選択します。
- メール脅威対策を設定します。

[ネットワーク脅威対策の次の設定を編集します？](#)

- ネットワーク脅威対策を有効または無効にします。

- ネットワーク脅威対策の設定を編集します。
- ネットワーク活動をブロックしないコンピュータの IP アドレスを指定します。

ファイアウォールの次の設定を編集します

- ファイアウォールを有効または無効にします。
- ファイアウォールを設定します。

• [先進の脅威対策] セクション

KSN の次の設定を編集します:

- [KSN 声明] をクリックして、Kaspersky Security Network 声明のテキスト全文を読みます。
- Kaspersky Security Network の使用を有効または無効にします。
- 拡張 KSN モードを有効または無効にします。
- クラウドモードを有効または無効にします。
- KSN プロキシの使用を有効または無効にします。
- KSN プロキシが使用できない場合、カスペルスキーのサーバの使用を有効または無効にします。

注意: Kaspersky Security Network と KSN プロキシをリモートコンピュータで使用可能なのは、Kaspersky Security Center 管理サーバーがプロキシサーバとして使用されている場合のみです。管理サーバーのプロパティの詳細は、[Kaspersky Security Center のヘルプ !\[\]\(0b3cb4e7b5e27760ecd51f5005862ccd_img.jpg\)](#)を参照してください。

ふるまい検知の次の設定を指定します

- ふるまい検知を有効または無効にします。
既定では、ふるまい検知は有効になっています。
- マルウェア活動の検知時に実行する処理を選択します。

脆弱性攻撃ブロックの次の設定を編集します

- 脆弱性攻撃ブロックを有効または無効にします。
- 脆弱性攻撃の検知時に実行する処理を選択します。

修復エンジンの次の設定を編集します

修復エンジンを有効または無効にします。

• [セキュリティコントロール] セクション

デバイスコントロールの次の設定を編集します

- デバイスコントロールを有効または無効にします。
- デバイスコントロールを設定します。

ウェブコントロールの次の設定を編集します:

- ウェブコントロールを有効または無効にします。

- ウェブコントロールに新しいルールを追加するには、[追加] をクリックします。
- リスト内に作成したルールを編集、削除、整理します。

- [データ暗号化] セクション

[FileVault ディスク暗号化の次の設定を編集します： ?](#)

- クライアントコンピュータで FileVault ディスク暗号化の管理を有効または無効にします。
- クライアントコンピュータの起動ディスクを暗号化または復号化します。
[FileVault ディスク暗号化の管理を有効にする] をオフにすると、管理者権限のあるユーザはシステム設定から Mac の起動ディスクを暗号化および復号化できます。
[FileVault ディスク暗号化の管理を有効にする] と [ディスクを暗号化する] をオンにすると、管理者権限のあるユーザがシステム設定から Mac の起動ディスクを復号化することはできません。
[FileVault ディスク暗号化の管理を有効にする] と [ディスクを復号化する] をオンにすると、管理者権限のあるユーザがシステム設定から Mac の起動ディスクを暗号化することはできません。

- [Detection and Response] セクション

[Managed Detection and Response の次の設定を編集します ?](#)

- Managed Detection and Response を有効または無効にします。
- 管理対象デバイスで Managed Detection and Response の有効化に使用する設定情報ファイルをインポートまたは削除します。

[次の Endpoint Detection and Response \(KATA\) 設定を指定します： ?](#)

- Endpoint Detection and Response (KATA) を有効または無効にします。
- サーバー接続の設定を指定し、TLS 証明書を追加します。
- KATA サーバーを追加します。

- [ローカルタスク] セクション

[次の外部ディスクのスキャン設定を指定します ?](#)

- 外部ディスクの接続時に Kaspersky Endpoint Security が実行する動作。
- 悪意のあるオブジェクトの検知時に Kaspersky Endpoint Security が実行する処理を指定します。

- [アップデート] セクション

[アップデートの次の設定を編集します： ?](#)

- ソフトウェアモジュールのアップデートを有効または無効にします。
- アップデート元を指定します。

- [詳細設定] セクション

[保護機能の次の設定を編集します： ?](#)

- クライアントコンピュータのリアルタイム保護を有効または無効にします。
- クライアントコンピュータの起動時に Kaspersky Endpoint Security の起動を有効または無効にします。
- 信頼ゾーンを設定します。
- 信頼済みアプリケーションを設定します。

- 検知するオブジェクトの種別を選択します。
- コンピュータがバッテリーで稼働している時、スケジュールされたタスクの起動を有効または無効にします。

次のネットワーク設定を編集します：

- プロキシサーバの使用を有効または無効にします。
- プロキシサーバのアドレスを指定します。
- ローカルアドレスに対するプロキシサーバの使用を有効または無効にします。
- プロキシサーバの認証に使用するユーザ名およびパスワードを指定します。
- 送受信する HTTPS トラフィックのスキャンを有効または無効にします。
- Mozilla Firefox ブラウザで暗号化された HTTPS トラフィックをチェックするための証明書ストアを選択します。
- 監視対象ポートを設定します。

次のレポートとバックアップの設定を編集します：

- 緊急以外のイベントもレポートに保存するオプションを有効または無効にします。
- 最近のイベントのみを保存するオプションを有効または無効にします。
- 指定された時間の経過後にイベントを削除するオプションを有効または無効にします。
- イベントを保存する期間を指定します。
- 指定された時間の経過後にバックアップからオブジェクトを削除するオプションを有効または無効にします。
- バックアップにオブジェクトを保存する期間を指定します。

ユーザインターフェイスの次の設定を編集します：

- イベント通知を有効または無効にします。
- Kaspersky Endpoint Security がユーザにイベントを通知する方法を選択します。
- メニューバーの Kaspersky Endpoint Security アイコンの表示を有効または無効にします。
- ユーザが、リモートコンピュータから Kaspersky Endpoint Security のメインウィンドウを表示してインターフェイスを使用できるようにするかを設定します。
- クライアントコンピュータの Kaspersky Endpoint Security アイコンのショートカットメニューで [終了] の表示を有効または無効にします。
- Kaspersky Security Center のイベントの表示に使用される言語を選択します。
- クライアントコンピュータのユーザで利用できる Kaspersky Endpoint Security の設定を編集します。
- パスワード保護を設定して、ユーザデバイスでの不要な操作を制限します。

7. [OK] をクリックして変更を保存し、ポリシーのプロパティウィンドウを閉じます。

ポリシーのステータスを変更する

ポリシーのステータスは、ポリシーの動作を定義します。ポリシーのステータスは、アクティブ、モバイルユーザ用、非アクティブのいずれかです。ポリシーのステータスは、ポリシーの設定で変更できます。

ポリシーのステータスを変更する

1. Kaspersky Security Center の管理コンソールを起動します。
2. [管理サーバ - <サーバ名>] フォルダを展開します。
3. コンソールツリーで、[管理対象デバイス] をクリックします。
4. 対象のクライアントコンピュータが含まれた管理グループを選択します。
5. 作業領域で、[ポリシー] タブを選択します。
6. ステータスを変更するポリシーを右クリックして、コンテキストメニューで [プロパティ] を選択します。
7. プロパティ：<ポリシー名> ウィンドウで、[全般] セクションを選択します。
8. [ポリシーのステータス] セクションで、次のいずれかのステータスを選択します：
 - **アクティブポリシー**：選択された管理グループにポリシーが常時適用されます。
 - **モバイルユーザーポリシー**：選択された管理グループが企業ネットワークから接続解除した時にポリシーが適用されます。
 - **非アクティブポリシー**：選択された管理グループにポリシーは適用されません。
9. [OK] をクリックして変更を保存し、**ポリシーのプロパティ** ウィンドウを閉じます。

KLP ファイルにポリシーをエクスポートする

カスタマイズしたポリシーをファイルにエクスポートして、そのポリシーを別の管理サーバーで使用できます。

[KLP ファイルにポリシーをエクスポートする](#)

1. Kaspersky Security Center の管理コンソールを起動します。
2. [管理サーバ - <サーバ名>] フォルダを展開します。
3. コンソールツリーで、[管理対象デバイス] をクリックします。
4. 対象のクライアントコンピュータが含まれた管理グループを選択します。
5. 作業領域で、[ポリシー] タブを選択します。
6. ポリシーを右クリックしてコンテキストメニューを表示し、[エクスポート] を選択します。
[名前を付けて保存] ウィンドウが表示されます。
7. ポリシーの KLP ファイルを保存するフォルダを選択します。
8. ファイル名を指定します。
9. [保存] をクリックして、選択したフォルダにファイルを保存します。

KLP ファイルからポリシーをインポートする

設定が定義された既存のポリシーをファイルからインポートできます。

[KLP ファイルからポリシーをインポートする](#)

1. Kaspersky Security Center の管理コンソールを起動します。
2. [管理サーバ - <サーバ名>] フォルダを展開します。
3. コンソールツリーで、[管理対象デバイス] をクリックします。
4. 対象のクライアントコンピュータが含まれた管理グループを選択します。
5. 作業領域で、[ポリシー] タブを選択します。

6. 次のいずれかの方法で、ファイルを選択するウインドウを開きます：

- **「ポリシーをファイルからインポート」** をクリックする。
- 作業領域の何も表示されていない場所を右クリックしてコンテキストメニューを開き、**「インポート」** を選択する。

7. ポリシーの KLP ファイルを選択して **「開く」** をクリックします。

作業領域のポリシーのリストに、追加されたポリシーが表示されます。

ポリシーのプロファイルの作成と管理

ポリシーのプロファイルは、特定の条件を満たした時に、クライアントコンピュータ上で有効となるポリシーの変数設定の名前付きセットです。プロファイルを有効にすると、ポリシーのプロファイルが有効になる直前にデバイスで有効になっていたポリシー設定が修正されます。

[ポリシーのプロファイルを作成する](#)

1. コンソールツリーで、ポリシーのプロファイルを作成する管理グループを選択します。

2. 作業領域で、**「ポリシー」** タブを選択します。

3. プロファイルを作成するポリシーのプロパティを、次のいずれかの方法で開きます：

- ポリシーの名前をダブルクリックする。
- ポリシー名を右クリックしてコンテキストメニューを開き、**「プロパティ」** を選択する。
- **「ポリシーの設定」** をクリックします。

4. ポリシーのプロパティウインドウで、**「ポリシーのプロファイル」** セクションを選択します。

5. 作業領域で、**「追加」** をクリックします。

6. **「ポリシープロファイルを割り当てる」** ウインドウで、ポリシーに関する情報を確認して **「次へ」** をクリックします。

新規ポリシープロファイルの作成時にこのウインドウを表示しない場合、**「次へ」** をクリックする前に **「次からこのウインドウを表示しない」** をオンにします。

7. **「ポリシーのプロファイル名」** ウインドウで、ポリシーのプロファイルを設定します：

- 新規ポリシープロファイルの名前を入力します。

注意： プロファイル名を 100 文字以上にすることはできません。

- **「ポリシープロファイルの状態」** セクションで、ポリシープロファイルを有効にするか無効にするかを選択します。
 - **「ポリシープロファイルの状態」** セクションのドロップダウンリストで、ポリシープロファイルの編集を許可するかどうかを選択します。
 - ポリシープロファイルに対して有効化ルールを設定する場合、**「新規ポリシープロファイルウィザードの終了後、ポリシープロファイルの有効化ルールの設定に進む」** をオンにします。
8. **「完了」** をクリックします。
9. **「新規ポリシープロファイルウィザードの終了後、ポリシープロファイルの有効化ルールの設定に進む」** を選択している場合は、新規ポリシープロファイル有効化ルールウィザードの手順を進めます。

作成したポリシープロファイルが、**ポリシーのプロパティ** の **「ポリシーのプロファイル」** セクションに表示されます。

[ポリシープロファイルの有効化ルールを作成する](#)

1. コンソールツリーで、ポリシーのプロファイルを有効化するルールを作成する管理グループを選択します。

2. 作業領域で、**「ポリシー」** タブを選択します。

3. ポリシーのプロパティを、次のいずれかの方法で開きます：

- ポリシーの名前をダブルクリックする。
- ポリシー名を右クリックしてコンテキストメニューを開き、**プロパティ** を選択する。
- **ポリシーの設定** をクリックします。

4. **ポリシーのプロパティ** ウィンドウで、**ポリシーのプロファイル** セクションを選択します。

5. 作業領域で、有効化ルールを作成するポリシープロファイルを選択し、**プロパティ** をクリックします。

ポリシーのプロファイルのプロパティ ウィンドウが開きます。

6. **有効化ルール** セクションを選択します。

7. 作業領域で、**追加** をクリックします。

新規ポリシープロファイル有効化ルールウィザードが開始します。

新規ポリシープロファイル有効化ルールウィザードの手順に従います。

ポリシーのプロファイルを編集する

1. コンソールツリーで、ポリシーのプロファイルを編集する管理グループを選択します。

2. 作業領域で、**ポリシー** タブを選択します。

3. プロファイルを編集するポリシーのプロパティを、次のいずれかの方法で開きます：

- ポリシーの名前をダブルクリックする。
- ポリシー名を右クリックしてコンテキストメニューを開き、**プロパティ** を選択する。
- **ポリシーの設定** をクリックします。

4. **ポリシーのプロパティ** ウィンドウで、**ポリシーのプロファイル** セクションを選択します。

5. 作業領域で、編集するポリシーのプロファイルを選択して **プロパティ** をクリックします。

ポリシーのプロファイルのプロパティ ウィンドウが開きます。

6. 必要に応じて、ポリシーを設定します：

- **全般** セクションでプロファイルの名前を変更するか、**プロファイルの有効化** をオンまたはオフにしてプロファイルを有効または無効にします。
- **有効化ルール** セクションで、有効化ルールを作成、編集、または削除します。
- **デバイス** セクションで、ポリシーのプロファイルを適用するデバイスを選択します。
- 該当するセクションでポリシーの設定を編集します。

7. **OK** をクリックします。

ポリシーのプロファイルが有効な場合、編集した設定は、クライアントコンピュータと管理サーバーの同期後に適用されます。ポリシーのプロファイルが無効な場合は、有効化ルールが適合した時に適用されます。

ポリシーのプロファイルにおける優先度を変更する

1. コンソールツリーで、ポリシープロファイルの優先度を変更する管理グループを選択します。

2. 作業領域で、**ポリシー** タブを選択します。

3. ポリシープロファイルの優先度を変更するポリシーのプロパティを、次のいずれかの方法で開きます：

- ポリシーの名前をダブルクリックする。
- ポリシー名を右クリックしてコンテキストメニューを開き、**プロパティ** を選択する。
- **ポリシーの設定** をクリックします。

4. ポリシーのプロパティウィンドウで、[ポリシーのプロファイル] セクションを選択します。
5. 作業領域で、優先度を変更するポリシープロファイルを選択します。
6.  または  をクリックして、選択したプロファイルの優先度を上げたり下げたりします。

[ポリシーのプロファイルを削除する](#)

1. コンソールツリーで、ポリシーのプロファイルを削除する管理グループを選択します。
2. 作業領域で、[ポリシー] タブを選択します。
3. プロファイルを削除するポリシーのプロパティを、次のいずれかの方法で開きます：
 - ポリシーの名前をダブルクリックする。
 - ポリシー名を右クリックしてコンテキストメニューを開き、[プロパティ] を選択する。
 - [ポリシーの設定] をクリックします。
4. ポリシーのプロパティウィンドウで、[ポリシーのプロファイル] セクションを選択します。
5. 作業領域で、削除するプロファイルを選択して [削除] をクリックします。

ポリシープロファイルの詳細は、[Kaspersky Security Center のヘルプ](#) を参照してください。

検知したオブジェクトのレポートを生成する

[検知したオブジェクトのレポートを生成する](#)

1. Kaspersky Security Center の管理コンソールを起動します。
 2. [管理サーバ - <サーバ名>] フォルダを展開します。
 3. コンソールツリーで、[管理対象デバイス] をクリックします。
 4. 対象のクライアントコンピュータが含まれた管理グループを選択します。
 5. [デバイス] タブを選択します。
 6. クライアントコンピュータのリストからコンピュータを選択します。
 7. 選択したコンピュータを右クリックしてコンテキストメニューを開き、[すべてのタスク] → [脅威レポートの表示] の順に選択します。
- 生成されたレポートは、ブラウザのウィンドウに表示されます。

クライアントコンピュータ上のアプリケーションによって検知されたオブジェクトに関するレポートを生成する他の方法は、[Kaspersky Security Center のヘルプ](#) を参照してください。

暗号化されたディスクの回復キーを取得する

クライアントコンピュータのユーザが資格情報を忘れたり失ったりして、暗号化されたディスクにアクセスできない場合、回復キーを取得できます。

[回復キーを取得](#)

1. Kaspersky Security Center の管理コンソールを起動します。
2. [管理サーバ - <サーバ名>] フォルダを展開します。
3. コンソールツリーで [詳細] フォルダの [データの暗号化と保護] サブフォルダを選択して、[暗号化されたドライブ] サブフォルダを選択します。
4. 作業領域で、暗号化されたディスクのあるデバイスを右クリックしてショートカットメニューを表示し、[macOSの回復キーを取得] を選択します。

回復キーが表示されたウィンドウが表示されます。

5. 任意の方法で回復キーを保存します。

クライアントコンピュータでこの回復キーを使用し、暗号化されたディスクにアクセスします。

Kaspersky Security Center Web コンソールおよび Cloud コンソールを経由する製品のリモート管理

Kaspersky Security Center Web コンソール (Web コンソール) は、組織のネットワークセキュリティの管理と保守に関連する主なタスクを集中的に実行するための Web アプリケーションです。Web コンソールは、ブラウザウィンドウで Kaspersky Endpoint Security を管理するためのユーザーインターフェイスを提供する Kaspersky Security Center のコンポーネントです。Kaspersky Security Center Web コンソールの詳細は、[Kaspersky Security Center のヘルプ](#) を参照してください。

Kaspersky Security Center Cloud コンソール (Cloud コンソール) は、組織のネットワークを保護および管理するためのクラウドベースのソリューションです。Kaspersky Security Center Cloud コンソールの詳細は、[Kaspersky Security Center Cloud コンソールのヘルプ](#) を参照してください。

Kaspersky Endpoint Security を、[製品のグラフィカルユーザーインターフェイス](#)、[Kaspersky Security Center 管理コンソール](#)または[コマンドライン](#)から管理することもできます。

Kaspersky Endpoint Security Web プラグインをインストールする

Kaspersky Endpoint Security Web プラグインにより、Kaspersky Endpoint Security と Kaspersky Security Center 間の対話が可能になります。Web プラグインは、Kaspersky Security Center Web コンソールがインストールされているデバイスにインストールする必要があります。Web プラグインの機能は、ブラウザで Kaspersky Security Center Web コンソールにアクセスできるすべての管理者が使用できます。

Web プラグインは次の方法でインストールできます：

- Kaspersky Security Center Web コンソールのクイックスタートウィザードを使用します。
Web コンソールを管理サーバーへの初回接続時に、Web コンソールは自動的にクイックスタートウィザードを実行するように要求します。Web コンソールインターフェイス ([**検出と導入**] → [**導入と割り当て**] → [**クイックスタートウィザード**]) でクイックスタートウィザードを実行することもできます。クイックスタートウィザードでは、インストールされているアップデートをダウンロードすることもできます。Kaspersky Security Center Web コンソールのクイックスタートウィザードの詳細は、[Kaspersky Security Center のヘルプ](#) を参照してください。
- 外部ソースから Web コンソールへの配布パッケージを使用して手動で行います。
Web プラグインをインストールするには、Web コンソールのインターフェイス ([**コンソール設定**] → [**Web プラグイン**]) に、Kaspersky Endpoint Security Web プラグインの配布パッケージの ZIP アーカイブを追加します。Web プラグインの配布パッケージは、カスペルスキーの Web サイトからダウンロードできます。

Kaspersky Endpoint Security Web プラグインを手動でインストールするには：

1. Kaspersky Security Center Web コンソールのメインウィンドウで、[**コンソール設定**] → [**Web プラグイン**] の順に選択します。
インストールされている Web プラグインのリストが開きます。

2. 次のいずれかの方法で、Kaspersky Endpoint Security Web プラグインのインストールを開始します：

- カスペルスキー製品の Web プラグインのリストからのインストール：
 - a. [**追加**] をクリックします。
インストール可能なすべてのカスペルスキー製品の Web プラグインのリストが開きます。新しいバージョンの Web プラグインがリリースされると、リストは自動的に更新されます。
 - b. リストで Kaspersky Endpoint Security for Mac 12.2 Web プラグインを見つけて、その名前をクリックします。
 - c. Web プラグインの説明が表示されたウィンドウで、[**プラグインのインストール**] をクリックします。
 - d. インストールが完了するまで待ってから、情報ウィンドウで [**OK**] をクリックします。
- 外部ソースからの Web プラグインのインストール (Web プラグインのインストールに必要なアーカイブは、配布キットに含まれています)：
 - a. [**ファイルから追加**] をクリックします。
 - b. 表示されるウィンドウで、Web プラグインの配布キットを含む ZIP アーカイブへのパスと、TXT 形式の署名ファイルへのパスを指定します。このファイルは、Web プラグインとともにアーカイブに含まれています。
 - c. [**追加**] をクリックします。
 - d. インストールが完了するまで待ってから、情報ウィンドウで [**OK**] をクリックします。

新しいプラグインは、インストールされている Web プラグインのリスト（[[コンソールの設定](#)] → [[Web プラグイン](#)]）に表示されます。

注意： Kaspersky Security Center 管理サーバーのプロパティで Kaspersky Endpoint Security 配布パッケージに含まれていない言語を選択した場合、使用許諾契約書と Kaspersky Security Center Web コンソールのインターフェイス全体が英語で表示されます。

ポリシーの作成

このセクションでは、Kaspersky Security Center Web コンソールと Cloud コンソールを使用して、Kaspersky Endpoint Security のポリシーを作成および設定する方法について説明します。

ポリシーは、アプリケーションの設定を決定するとともに、管理グループ内のコンピュータにインストールされたアプリケーションの設定へのアクセスを管理します。各アプリケーションについて個別にポリシーを作成する必要があります。各管理グループのコンピュータにインストールされたアプリケーション向けに複数のポリシーを作成できますが、各管理グループ内で1つのアプリケーションについて一度に適用されるポリシーは1つのみです。

注意： ポリシーを作成、設定時に、[[強制適用](#)] スイッチを使用して、ポリシー内の任意の設定のグループに対する変更を禁止または許可できます。

[ポリシーの作成](#)

1. 左の [[デバイス](#)] セクションで、[[ポリシーとプロファイル](#)] セクションを選択します。
2. [[追加](#)] をクリックします。
3. ポリシーを作成するアプリケーションを選択して、[[Next](#)] をクリックします。
[[新規ポリシー](#)] ウィンドウが表示されます。
4. [[全般](#)] タブでポリシー名を指定し、ポリシーの状態とポリシー設定の継承オプションを設定します。
5. [[アプリケーション設定](#)] タブで、ポリシー適用時にクライアントコンピュータの Kaspersky Endpoint Security に適用されるアプリケーション設定を設定します。
6. [[保存](#)] をクリックします。

カスタムポリシーでは、次の操作を実行できます：

- ポリシーの作成
- ポリシーの設定
- あるグループから別のグループへのポリシーのコピーおよび移動
- ポリシーの削除
- ポリシーのステータスの変更

Kaspersky Security Center Web コンソールのポリシーの詳細は、[Kaspersky Security Center のヘルプ](#) を参照してください。

Kaspersky Security Center Cloud コンソールのポリシーの詳細は、[Kaspersky Security Center Cloud コンソールのヘルプ](#) を参照してください。

注意： Kaspersky Security Center Web コンソールと Cloud コンソールを使用して Kaspersky Endpoint Security ポリシーのポリシープロファイルを作成した後、設定がクライアントコンピュータに正しく適用されていることを確認する必要があります。

先進の脅威対策の設定

[[先進の脅威対策](#)] セクションでは、クライアントコンピュータ上の Kaspersky Endpoint Security が Kaspersky Security Network への参加をするかどうかを選択し、KSN プロキシの使用を設定できます。

必要に応じて次のことを行います：

- [[KSN 声明](#)] をクリックして、Kaspersky Security Network 声明のテキスト全文を読む
- [[KSN 声明](#)] をクリックして、Kaspersky Security Center から提供される KSN インフラストラクチャに関する情報を表示します。

注意：既定では、グローバル KSN インフラストラクチャが、Kaspersky Security Center で使用されます。Kaspersky Security Center Web コンソールを介して Kaspersky Endpoint Security を管理している場合、Kaspersky Security Center の設定に応じて、Kaspersky Security Network の代わりに Kaspersky Private Security Network への参加を行うことができます。Kaspersky Security Center Cloud コンソールを介して Kaspersky Endpoint Security を管理している場合、Kaspersky Private Security Network への参加はできません。Kaspersky Private Security Network への参加に関する詳細は、[Kaspersky Security Center のヘルプ](#) を参照してください。

- Kaspersky Security Network の使用を有効または無効にする
- 拡張 KSN モードを有効または無効にする
- クラウドモードをオンまたはオフにします。
- KSN プロキシの使用を有効または無効にします。
- KSN プロキシが使用できない場合、カスペルスキーのサーバの使用を有効または無効にします。

注意：Kaspersky Security Center Web コンソールを介して Kaspersky Endpoint Security を管理している場合、Kaspersky Security Network と KSN プロキシをリモートコンピュータで使用可能なのは、Kaspersky Security Center 管理サーバーがプロキシサーバとして使用されている場合のみです。管理サーバーのプロパティの詳細は、[Kaspersky Security Center のヘルプ](#) を参照してください。
Kaspersky Security Center Cloud コンソールを使用して Kaspersky Endpoint Security を管理する場合は、Windows オペレーティングシステムを実行しているディストリビューションポイントを経由して、リモートコンピュータ上で Kaspersky Security Network と KSN プロキシを使用できます。

ポリシーの設定で、Kaspersky Security Center によってグローバル KSN インフラストラクチャが使用されており、かつ、Kaspersky Security Network への参加を選択すると、ポリシーが適用されたクライアントコンピュータにおける Kaspersky Endpoint Security の統計情報が自動的にカスペルスキーに送信され、それらのコンピュータをより強力に保護できるようになります。

注意：カスペルスキーでは、お客様の明確な同意がない限り、いかなる個人情報の受信、処理、保管も行いません。

グローバル KSN インフラストラクチャの Kaspersky Security Network の使用時にカスペルスキーに提供されるデータ

[Kaspersky Security Network] スイッチを有効にし、[拡張 KSN モード] スイッチを無効にすると、クライアントコンピュータで実行中の本製品がカスペルスキーに次のデータを提供します：

- 適用されているライセンスの情報：ライセンスの種別および有効期間、ライセンスの有効期限までの日数、ライセンスの購入元である代理店の識別子、地域のアクティベーションセンターの識別子、アクティベーションコードのチェックサム、SHA1 アルゴリズムを使用して計算されたチケットボディのハッシュ、ライセンスチケットの作成日時、ライセンス情報の識別子、ライセンスチケットの識別子、ライセンスチケットのシーケンスの識別子、ユーザのコンピュータの一意な識別子、ライセンスチケットが有効になった日付、ライセンスチケットの有効期限、ライセンスチケットの現在のステータス、チケットヘッダーのバージョン、ライセンスのバージョン、チケットヘッダーの署名に使用された証明書の識別子、ライセンスファイルのチェックサム、チケットヘッダーの署名元のシリアル番号、認証トークン。
- インストールされた本ソフトウェアの詳細バージョン。

インストールされた本ソフトウェアの種別。ソフトウェアアップデートの ID。評価サービスの ID。プロトコルタイプの ID。地域のアクティベーションセンターの ID。本ソフトウェアのサービスの決定のうち取り消されたもののリストのバージョン。トリガーされた本ソフトウェアの定義データベースのレコードの ID。トリガーされた本ソフトウェアの定義データベースのレコードのタイムスタンプ。トリガーされた本ソフトウェアの定義データベースのレコードの種別。本ソフトウェアのコンピュータへのインストールのインスタンスの一意な ID。ライセンスがアクティベートされた日付。ライセンスの有効期限日。ライセンスの識別子。本ソフトウェアが使用中のライセンスのステータス。処理中のオブジェクトのチェックサム種別。検知されたマルウェアの名前、ユーザのコンピュータまたはデータに損害を与える目的で使用される可能性がある正規のソフトウェアの名前。処理中のオブジェクトのチェックサム。本ソフトウェアのアクティベーションコードのチェックサム。本ソフトウェアの詳細バージョン。一意のデバイス ID。本ソフトウェアの ID。本ソフトウェアのライセンス情報ファイルのチェックサム。本ソフトウェアのライセンスの提供に使用された情報形式の ID。本ソフトウェアのライセンスチケットのヘッダーへの署名に使用される証明書の識別子。本ソフトウェアのライセンスチケットの作成日時。本ソフトウェアのライセンスチケットのチェックサム。本ソフトウェアのライセンスチケットのバージョン。本ソフトウェアのアクティベーションコードのバージョン。権利者のインフラストラクチャへのリクエストに含まれるデータの形式。使用中のライセンスチケットの ID。本ソフトウェアのコンポーネントの ID。本ソフトウェアの動作の結果。エラーコード。アクセスされた Web サービスのアドレス (URL、IP)。ポート番号。Web サービスのリクエスト元の URL (リファラー)。証明書の公開鍵。スキャンされたオブジェクトのデジタル証明書のサムプリントとハッシュアルゴリズム。

[Kaspersky Security Network] と [拡張 KSN モード] のスイッチを有効にすると、クライアントコンピュータで実行中の本製品がカスペルスキーに次のデータを提供します：

- コンピュータにインストールされているオペレーティングシステム (OS) やサービスパックのバージョンに関する情報、OS カーネルファイルのバージョンおよびチェックサム (MD5、SHA2-256、SHA1)、OS 実行モードの識別子。OS のバージョン、OS のビルド番号、OS のアップデート番号、OS のエディション、OS のエディションに関する詳細情報。OS のサービスパックのバージョン OS の起動日時。ふるまい分析のサブシステムにおける OS 動作に関するイベントの処理遅延時間。現在の種別の遅延された OS 動作イベントの数。プロアクティブディフェンスのサブシステムにおける OS 動作に関するイベントの処理遅延時間。処理された OS 動作イベントの数。処理された OS 同期動作イベントの数。現在の種別のすべての OS 動作イベントの合計遅延時間。持続的イベントを記憶するサブシステム

における、OS 動作に関するイベントの処理遅延時間。すべての OS 動作イベントの合計遅延。待機中の OS 同期動作イベントの数。OS 内の動作イベントを受信した日時。

- 以前、OS の再起動が失敗した履歴：再起動に失敗した回数。
- インストールされている本製品に関する情報およびアンチウイルス保護状況：ソフトウェアのインストール識別子（PCID）本ソフトウェアの定義データベースのレコードのバージョン、コンピューター上にインストールされたアプリケーションのインスタンスの一意な識別子、アプリケーションの種別、アプリケーション種別の識別子、インストールされたアプリケーションの詳細バージョン、アプリケーションの設定のバージョンの識別子、コンピューター種別の識別子、アプリケーションがインストールされたコンピューターの一意な識別子、権利者のサービスにおける一意なユーザー識別子、言語および動作状況、インストールされたソフトウェアコンポーネントのバージョンと動作状況、権利者のサービスに接続するために使用されたプロトコルのバージョン、インストールされた本ソフトウェアの詳細バージョン。インストールされた本ソフトウェアの種別。ソフトウェアアップデートの ID。評価サービスの ID。プロトコルタイプの ID。地域のアクティベーションセンターの ID。本ソフトウェアのサービスの決定のうち取り消されたもののリストのバージョン。トリガーされた本ソフトウェアの定義データベースのレコードの ID。トリガーされた本ソフトウェアの定義データベースのレコードのタイムスタンプ。トリガーされた本ソフトウェアの定義データベースのレコードの種別。本ソフトウェアのコンピューターへのインストールのインスタンスの一意な ID。ライセンスがアクティベートされた日付。ライセンスの有効期限日。ライセンスの識別子。本ソフトウェアが使用中のライセンスのステータス。処理中のオブジェクトのチェックサム種別。検知されたマルウェアの名前、ユーザのコンピューターまたはデータに損害を与える目的で使用される可能性がある正規のソフトウェアの名前。処理中のオブジェクトのチェックサム。本ソフトウェアのアクティベーションコードのチェックサム。本ソフトウェアの詳細バージョン。本ソフトウェアの ID。本ソフトウェアのライセンス情報ファイルのチェックサム。本ソフトウェアのライセンスの提供に使用された情報形式の ID。本ソフトウェアのライセンスチケットのヘッダーへの署名に使用される証明書の識別子。本ソフトウェアのライセンスチケットの作成日時。本ソフトウェアのライセンスチケットのチェックサム。本ソフトウェアのライセンスチケットのバージョン。本ソフトウェアのアクティベーションコードのバージョン。権利者のインフラストラクチャへのリクエストに含まれるデータの形式。使用中のライセンスチケットの ID。本ソフトウェアのコンポーネントの ID。本ソフトウェアの動作の結果。エラーコード。アクセスされた Web サービスのアドレス（URL、IP）。ポート番号。Web サービスのリクエスト元の URL（リファラー）。定義データベースのアップデートと適用のサイクル数。定義データベースが最後にアップデートおよび適用された日時。本ソフトウェアの定義データベースの公開日時。本ソフトウェアのコンポーネントのバージョン。ソフトウェアアップデートの ID。インストールされた本ソフトウェアの種別。システムウォッチャーの開始日時。本ソフトウェアのインストール日時。システムウォッチャーによって統計が送信される確率。システムウォッチャーによる標準処理時間よりも長い時間がかかったイベントのコード。システムウォッチャーによる標準処理時間を超えたイベントのデータベース処理時間。システムウォッチャーによるイベントの処理に許可される最大時間。システムウォッチャーによる標準処理時間を超えたイベントの処理時間。システムウォッチャーによる標準処理時間よりも長い時間がかかったイベントの総数。
- 処理したすべてのオブジェクトおよび操作に関する情報：処理中のオブジェクトに対する本ソフトウェアの判定、ディレクトリコード、処理中のオブジェクトのサイズ、処理中のオブジェクトのチェックサム（SHA256）、システムウォッチャーを使用して検知されたソフトウェアの数、システムウォッチャーでソフトウェアを検知した日時、検知の特性、トリガーされた本ソフトウェアの定義データベースのレコードの ID。システムウォッチャーでソフトウェアを検知した理由、処理中のオブジェクトのチェックサム（MD5）、モジュールの整合性チェックの結果、処理中のオブジェクトの名前、トリガーされた本ソフトウェアの定義データベースのレコードの種別、処理中のオブジェクトへのパス。スキャンしたオブジェクトの製造元の名前、スキャンの日時、URL およびダウンロードされたリファラーのアドレス、スキャンされたファイルのサイズおよびパス、アーカイブかどうかのフラグ、ファイルの作成日時、圧縮されていた場合はバッカーの名前、サイズおよびチェックサム（MD5、SHA2-256）、ファイルのエントロピー、ファイルの種別、ファイル種別コード、ファイルが実行可能であるかどうかのフラグ、識別子および形式、オブジェクトのチェックサム（MD5、SHA2-256）、オブジェクトの追加チェックサムの種別および値、オブジェクトのデジタル署名（証明書）に関するデータ：証明書の発行元に関する情報、前回の統計が送信されてからオブジェクトが実行された回数、本製品のスキャンタスクの識別子、オブジェクトの評価に関する情報の受信手段、TARGET フィルターの値、適用可能な検知技術の技術的パラメータ。処理中のオブジェクトへのパス。ディレクトリコード。
- 実行ファイルの場合：ファイルセクションの情報量、評価の検証フラグまたはファイルの署名フラグ、検証対象のオブジェクトに読み込まれたアプリケーションの名前、種別、ID 種別、チェックサム（MD5）およびサイズ、アプリケーションのパスおよびテンプレートのパス、自動実行リストの署名、エントリの日時、属性のリスト、圧縮ソフトウェアの名前、アプリケーションのデジタル署名に関する情報：発行者の証明書、アップロードされたファイルの MIME 形式での名前、ファイルが作成された日時。
- 実行中のアプリケーションおよびそのモジュールに関する情報：実行中のファイルのチェックサム（MD5、SHA2-256）、ファイルのサイズ、属性、作成日時、圧縮ソフトウェアの名前（ファイルが圧縮されている場合）、ファイル名、システム上で実行されているプロセスに関する情報（プロセス ID（PID）、プロセス名、プロセスを開始したアカウントに関する情報、プロセスを開始したアプリケーションおよびコマンド、プロセスのファイルへの完全パスおよび開始したコマンドライン、プロセスが属するアプリケーションの説明（アプリケーション名および配信元の情報）、使用されるデジタル証明書およびそれらの正当性を検証するために必要な情報またはファイルのデジタル署名が存在しない旨のフラグ）、プロセスに読み込まれたモジュールの情報：名前、サイズ、種別、作成日、属性、チェックサム（MD5、SHA2-256、SHA1）およびパス、PE ファイルのヘッダー情報、圧縮ソフトウェア名（ファイルが圧縮されている場合）、統計情報の有効性および使用可否に関する情報、送信される統計情報の生成条件の識別子。
- 脅威または脆弱性が検知された場合、検知されたオブジェクトに関する情報に加え、次の情報が提供されます：定義データベース中のレコードの識別子、バージョンおよび種別、カスペルスキーの分類による脅威名、定義データベースの最終アップデート日時、実行ファイルの名前、脅威が検知された URL をリクエストしたアプリケーションのファイルのチェックサム（MD5）、検知した脅威の IP アドレス（IPv4 または IPv6）、脆弱性の識別子および脅威レベル、脅威を検知した Web ページの URL およびリファラー。
- 悪意のある可能性があるオブジェクトが検知された場合、プロセスのメモリ内のデータに関する情報が提供されます。
- ネットワーク攻撃の情報：攻撃元コンピュータの IP アドレスおよびユーザのコンピュータ上でネットワーク攻撃の標的にされたポート番号、攻撃プロトコルの ID、名前および攻撃種別。
- ネットワーク接続に関する情報：ポートを開いたプロセスを起動したファイルのバージョンおよびチェックサム（MD5、SHA2-256、SHA1）、プロセスのファイルのパスおよびデジタル署名、ローカルおよびリモートの IP アドレス、ローカルおよびリモート接続のポート番号、接続状況、ポートが開かれた時刻。
- 危険なオブジェクトまたは疑わしいオブジェクトを検知した Web ページの URL および IP アドレス、この URL をリクエストしたファイルの名前、サイズおよびチェックサム、識別子、検知結果の決定基準に使用されたルールの重み係数および度数、攻撃の目的に関する情報。

- インストール済み本ソフトウェアおよび定義データベースのアップデートに関する情報：アップデートタスクの完了状況、アップデート中に発生した可能性のあるエラーの種別、失敗したアップデートの数、アップデートを実行した本ソフトウェア機能の識別子。
- **Kaspersky Security Network (KSN)** の使用に関する情報：KSN の識別子、本ソフトウェアの識別子、本ソフトウェアの詳細バージョン、個人を特定できないようにしたお客様のデバイスの IP アドレス、KSN へのリクエストの実行品質を示す指数、KSN 用パケットの処理品質を示す指数、KSN へのリクエストの件数およびリクエストの種別に関する情報、統計情報の送信を開始した日時と終了した日時、KSN 設定のアップデートに関する情報：アクティブな設定の識別子、受信した設定の識別子、設定のアップデートのエラーコード。
- イベントに関するシステムログ内の情報：イベントのタイムスタンプ、イベントが検知されたログの名前、イベントの種別およびカテゴリ、イベントの発生源の名前およびイベントの説明。
- ファイルおよび URL の評価決定に関する情報：評価が要求された URL とその参照元、接続のプロトコルタイプ、アプリケーション種別の内部識別子、使用されているポートの番号、ユーザ識別子、スキャンされたファイルのチェックサム (MD5)、検知された脅威の種別、脅威の検知に使用した記録に関する情報 (定義データベースの記録の識別子、記録のタイムスタンプと種別)。証明書
の公開鍵。スキャンされたオブジェクトのデジタル証明書のサムプリントとハッシュアルゴリズム。
- 本ソフトウェアの地域分布に関する情報：本ソフトウェアのインストールおよびアクティベーションの日時、本ソフトウェアのアクティベーション用のライセンスを提供した代理店の識別子、本ソフトウェアの識別子、本ソフトウェアの言語版の識別子、本ソフトウェアに適用されたライセンスの識別番号、KSN に参加しているかどうかのフラグ。
- 適用されているライセンスの情報：ライセンスの種別および有効期間、ライセンスの有効期限までの日数、ライセンスの購入元である代理店の識別子、地域のアクティベーションセンターの識別子、アクティベーションコードのチェックサム、SHA1 アルゴリズムを使用して計算されたチケットボディのハッシュ、ライセンスチケットの作成日時、ライセンス情報の識別子、ライセンスチケットの識別子、ライセンスチケットのシーケンスの識別子、ユーザのコンピュータの一意な識別子、ライセンスチケットが有効になった日付、ライセンスチケットの有効期限、ライセンスチケットの現在のステータス、チケットヘッダーのバージョン、ライセンスのバージョン、チケットヘッダーの署名に使用された証明書の識別子、ライセンスファイルのチェックサム、チケットヘッダーの署名元のシリアル番号、認証トークン。
- コンピュータにインストールされているハードウェアに関する情報：搭載または接続された装置の種別、名前、機種名、ファームウェアのバージョン、パラメータ。
- 端末に関する情報：端末の識別子。
- ウェブコントロール機能の動作に関する情報：
機能のバージョン、当該カテゴリに分類された理由および関連情報、分類された URL、ブロックまたは分類されたオブジェクトのホストの IP アドレス。

ポリシーの設定で、**Kaspersky Security Center** によってプライベート **KSN** インフラストラクチャが使用されており、かつ、**Kaspersky Security Network** への参加を選択すると、**Kaspersky Endpoint Security** は、ポリシーが適用されたクライアントコンピュータからの統計情報をカスペルスキーに送信しなくなります。

脅威対策の設定

「**脅威対策**」セクションでは、次のコンポーネントが設定できます：

- [ファイル脅威対策](#)
- [ウェブ脅威対策](#)
- [ネットワーク脅威対策](#)

対応するリンクをクリックして、ウィンドウを開き、コンポーネントの設定を設定できます。

ファイル脅威対策の設定

「**ファイル脅威対策**」ウィンドウで、必要に応じて次を設定します：

- ファイル脅威対策を有効または無効にする。
既定では、ファイル脅威対策は有効になっています。
- 保護範囲の作成
- 悪意のあるオブジェクトの検知時に実行する処理を選択します。
- **Kaspersky Endpoint Security** で新しいファイルと変更されたファイルのみをスキャンするか、すべてのファイルをスキャンするかを選択します。
- クライアントコンピュータで、読み取り専用ボリュームのスキャンをスキップするかどうかを選択します。
- **Kaspersky Endpoint Security** でファイルのスキャン中に iSwift テクノロジーを使用するかどうかを選択します。

注意：iSwift を使用すると、Kaspersky Endpoint Security は特別なアルゴリズムを使用して特定のオブジェクトをスキャンから除外し、スキャン速度を向上させることができます。

- Kaspersky Endpoint Security でスキャンするファイルの種類を選択します。
- Kaspersky Endpoint Security で複合ファイルに対して実行するアクションを選択します。

ウェブ脅威対策の設定

〔ウェブ脅威対策〕 ウィンドウで、必要に応じて次の設定を行います：

- ウェブ脅威対策を有効または無効にする。
既定では、ウェブ脅威対策は有効になっています。
- Web トラフィックで悪意のあるオブジェクトを検知した時に実行する処理を選択します。
- 信頼する Web アドレスのリストの作成または編集を行うには。

ネットワーク脅威対策の設定

〔ネットワーク脅威対策〕 ウィンドウで、必要に応じて次の設定を行います：

- ネットワーク脅威対策を有効または無効にする。
既定では、ネットワーク脅威対策が有効になっています。
- 攻撃元コンピュータのブロックを有効または無効にする。
- ネットワーク活動が Kaspersky Endpoint Security によってブロックされないリモートコンピュータの IP アドレスのリストを作成または編集します。

セキュリティコントロールの設定

〔セキュリティコントロール〕 セクションで、必要に応じて次の設定を行います：

- ウェブコントロールを有効または無効にする

注意：ウェブコントロールをオンにして危険な Web サイトをブロックすると、〔ウェブコントロールが有効です〕という通知がリモートコンピュータのプロテクションセンターに表示されます。
新規ポリシーウィザードのウィンドウの〔ネットワーク〕セクションで〔セキュアな接続 (HTTPS) をチェック〕スイッチをオンにすると、リモートコンピュータ上でウェブコントロールによってブロックされる Web サイトにユーザがアクセスすると通知が表示されます。

- ユーザのコンピュータ上のウェブコントロールによって監視および管理する URL や Web サイトカテゴリを設定するためのルールを追加します。
- リスト内に作成したルールを編集、削除、整理します。

ルールの並び順に従って、Kaspersky Endpoint Security が判断する適用の優先順位が決定されます。

データ暗号化の設定

〔データ暗号化〕 セクションでは、クライアントコンピュータの起動ディスクの暗号化をオンまたはオフにして、不正なユーザが機密データにアクセスするのを防ぎます。既定では、FileVault ディスク暗号化は無効になっています。

Detection and Response の設定

〔Detection and Response〕 セクションでは、次のコンポーネントを設定できます：

- [Managed Detection and Response](#)
- [Endpoint Detection and Response](#)
- [Endpoint Detection and Response \(KATA\)](#)

対応するリンクをクリックして、ウィンドウを開き、コンポーネントの設定を設定できます。

Managed Detection and Response の設定

〔Managed Detection and Response〕 ウィンドウで、必要に応じて次を実行します：

- **Managed Detection and Response** コンポーネントを有効または無効にします。
- **MDR 設定情報ファイル**をインポートまたは削除します。

Managed Detection and Response コンポーネントは、**Kaspersky Managed Detection and Response** サービスと対話します。このサービスは、組織を標的とする脅威を継続的に探索、検知、排除します。

既定では、**Managed Detection and Response** は無効になっています。

Endpoint Detection and Response の設定

「**Endpoint Detection and Response**」 ウィンドウで、必要に応じて次を実行します：

- **Endpoint Detection and Response** コンポーネントを有効または無効にします。
- ユーザのデバイスのネットワーク分離を設定します。
 - ネットワーク分離を自動的にオフにするまでの遅延を指定します。
 - ネットワーク分離の除外を設定します。
- 実行防止を有効または無効にします。
- 禁止されたオブジェクトを実行したり開いたりすると実行される処理を選択します。
- 実行防止ルールの一覧を作成します。
- **Cloud Sandbox** を有効または無効にします。

Endpoint Detection and Response コンポーネントは、脅威の自動検知と、これらの脅威に対応する能力を組み合わせ、新しい脆弱性攻撃、ランサムウェア、ファイルレス攻撃、正規のシステムツールを使用した方法などの高度な攻撃に対抗します。

既定では、**Endpoint Detection and Response** は無効になっています。

Endpoint Detection and Response (KATA) の設定

「**Endpoint Detection and Response (KATA)**」 ウィンドウで、必要に応じて次の操作を実行します：

- **Endpoint Detection and Response (KATA)** コンポーネントを有効または無効にします。
- サーバー接続を設定します。
 - **KATA** サーバーの応答タイムアウト期間を指定します。
 - **TLS** 証明書を追加して、信頼できる接続を設定します。
 - **Kaspersky Endpoint Security** が **KATA** サーバーへの接続に相互認証を使用するかどうかを選択します。
 - パスワードで保護された暗号化コンテナをロードして、相互認証を有効にします。
- **KATA** サーバーを追加します。
- **Kaspersky Endpoint Security** が **KATA** サーバーに送信されるパケットに **TTL** を使用するかどうかを選択します。
- **KATA** サーバーにデータを送信するための設定を指定します。
- **Kaspersky Endpoint Security** によって **KATA** サーバーに送信されるイベントの数を制限します。

Endpoint Detection and Response (KATA) コンポーネントは、**Kaspersky Anti Targeted Attack Platform** ソリューションとの対話を促進し、標的型攻撃、高度な持続的脅威、ゼロデイ攻撃などの高度な脅威を迅速に検知します。

既定では、**Endpoint Detection and Response (KATA)** は無効になっています。

アップデートの設定

「**アップデート**」 セクションで、必要に応じて次を行います：

- ソフトウェアモジュールのアップデートを有効または無効にする。
- **Kaspersky Endpoint Security** のアップデートに使用されるアップデート元を追加または削除する。

詳細設定

「**詳細設定**」セクションで、必要に応じて次を実行します：

- クライアントコンピュータのオペレーティングシステムの保護を設定します。
- 検知するオブジェクトの種別を選択します。
- コンピュータがバッテリーで稼働している時、スケジュールされたタスクの起動を有効または無効にします。
- レポートの生成および保存を設定します。
- バックアップへのオブジェクトの保存を設定します。
- クライアントコンピュータのユーザと **Kaspersky Endpoint Security** の対話を設定します。
- プロキシサーバへの接続を設定します。
- 送受信する HTTPS トラフィックのスキャンを有効または無効にします。
- **Mozilla Firefox** ブラウザで暗号化された HTTPS トラフィックをチェックするための証明書ストアを選択します。
- 監視対象ポートを設定します。
- **Kaspersky Endpoint Security** で監視しない、信頼するファイル、フォルダ、アプリケーションのリストを編集します。

タスクの作成

このセクションでは、**Kaspersky Security Center Web** コンソールと **Cloud** コンソールを使用して、**Kaspersky Endpoint Security**が、**Kaspersky Security Center**によって管理されるクライアントコンピュータやコンピュータグループに対して実施するタスクを作成および設定する方法について説明します。

タスクとは、**Kaspersky Endpoint Security** がクライアントコンピュータで実行する、設定可能な処理のセットのことです。

Kaspersky Security Center Web コンソールおよび **Cloud** コンソールでは、次のタスクを作成できます：

- スキャン
- アップデート
- ロールバック
- ライセンスの追加

タスクの作成

1. 左の「**デバイス**」セクションで、「**タスク**」セクションを選択します。
2. 「**追加**」をクリックします。
タスク追加ウィザードが起動します。
3. 「**アプリケーション**」ドロップダウンリストから、「**Kaspersky Endpoint Security for Mac 12.2**」を選択します。
4. 「**タスク種別**」ドロップダウンリストで、作成するタスクを選択します。
5. 必要に応じて「**タスク名**」フィールドでタスク名を編集します。
6. タスクを割り当てるデバイスを選択します。
7. 選択したタスク種別を設定します。
8. 「**完了**」をクリックして、タスクの追加ウィザードを完了します。

注意：「**タスク作成の完了**」ウィンドウで「**タスクの作成が完了したらタスクの詳細を表示する**」オンにすると、既定のタスク設定の変更に進むことができます。このチェックボックスを選択しない場合、タスクは既定の設定で作成されます。既定のタスク設定は後からいつでも変更できます。

タスクに対して実行可能な操作は次の通りです：

- タスクの開始と停止。

- タスク設定の編集。
- タスクの進行状況の追跡。
- あるグループから別のグループへのタスクのコピーおよび移動。
- タスクの削除。

Kaspersky Security Center Web コンソールのタスクの詳細は、[Kaspersky Security Center のヘルプ](#) を参照してください。

Kaspersky Security Center Cloud コンソールのタスクの詳細は、[Kaspersky Security Center Cloud コンソールのヘルプ](#) を参照してください。

スキャンタスクの設定の編集

「**アプリケーション設定**」タブで、リモートコンピュータ上の Kaspersky Endpoint Security の**スキャン**タスクを設定できます。

[スキャンタスクの設定を開きます。](#)

1. 「**デバイス**」 → 「**タスク**」の順に選択します。
2. 「**スキャン**」タスク種別のタスクをダブルクリックします。
3. 「**アプリケーション設定**」タブをクリックします。

必要に応じて次を実行できます：

- スキャン範囲を定義します。
- 感染したオブジェクトの検知時に Kaspersky Endpoint Security が実行する処理を指定します。
- Kaspersky Endpoint Security で、スキャンタスクの実行時にスキャンするファイルの種類を選択します。
- スキャンのパフォーマンスを設定します。
- Kaspersky Endpoint Security で分析する複合ファイルを選択します。

注意：Kaspersky Endpoint Security は、OneDrive や iCloud ストレージ、その他のクラウドストレージにあるファイルをスキャンしません。これらのファイルをスキャン範囲から除外してください。そうしないと、スキャンタスクが「感染したファイルが削除されませんでした」というエラーで終了する可能性があります。

ライセンスの追加タスクの設定の編集

「**アプリケーション設定**」タブで、リモートコンピュータ上の Kaspersky Endpoint Security の**ライセンスの追加**タスクを設定できます。

[ライセンスの追加タスクの設定を開きます。](#)

1. 「**デバイス**」 → 「**タスク**」の順に選択します。
2. 「**ライセンスの追加**」タスク種別のタスクをダブルクリックします。
3. 「**アプリケーション設定**」タブをクリックします。

必要に応じて次を実行できます：

- 現在のライセンスを予備のライセンスにします。
- ユーザのコンピュータで Kaspersky Endpoint Security をアクティベートするための別のライセンスを選択します。
- Kaspersky Security Center リポジトリに新しいライセンス情報を追加します。

アップデートタスクの設定

「**アプリケーション設定**」タブで、リモートコンピュータ上の Kaspersky Endpoint Security の**アップデート**タスクを設定できます。

[アップデートタスクの設定を開きます。](#)

1. [デバイス] → [タスク] の順に選択します。
2. [アップデート] タスク種別のタスクをダブルクリックします。
3. [アプリケーション設定] タブをクリックします。

カスペルスキーのアップデートサーバが、Kaspersky Endpoint Security のアップデートの主な入手元です。アップデート元には、ディストリビューションポイント、ローカルフォルダおよびその他の Web サーバを使用することもできます。

Kaspersky Security Center Web コンソールを通して Kaspersky Endpoint Security を管理している場合、アップデート元のリストには既定でカスペルスキーのアップデートサーバと Kaspersky Security Center サーバが含まれています。Kaspersky Endpoint Security は、最初に Kaspersky Security Center サーバから、次にカスペルスキーのアップデートサーバからアップデートをダウンロードします。

Kaspersky Security Center Cloud コンソールを通して Kaspersky Endpoint Security を管理している場合、アップデート元のリストには既定でカスペルスキーのアップデートサーバとディストリビューションポイントが含まれています。Kaspersky Endpoint Security は、最初にディストリビューションポイントから、次にカスペルスキーのアップデートサーバからアップデートをダウンロードします。ディストリビューションポイントの詳細は、[Kaspersky Security Center のヘルプ](#) を参照してください。

必要に応じて次を実行できます：

- ソフトウェアモジュールのアップデートを有効または無効にする。
- Kaspersky Endpoint Security のアップデートに使用されるアップデート元を追加または削除する。

暗号化されたドライブの回復キーを取得する

クライアントコンピュータのユーザが認証情報を忘れたり紛失したりして、暗号化されたドライブにアクセスできない場合、回復キーを取得できます。

[回復キーを取得](#)

1. Kaspersky Security Center Web コンソールまたは Cloud コンソールのウインドウの右下隅にある管理者アカウント名をクリックします。
2. [インターフェイスのオプション] を選択します。
3. 開いたダイアログで、[データ暗号化と保護を表示] スイッチをオンにして、データ暗号化の管理を有効にし、[保存] をクリックします。
4. [操作] → [データ暗号化と保護] → [暗号化されたデバイス] の順に選択します。
暗号化されたデバイスのリストを開きます。
5. 暗号化されたドライブがあるデバイスに隣接するチェックボックスを選択します。
6. [オフラインモードでのデバイスのアクセスを許可する] をクリックします。
7. [オフラインモードでのデバイスのアクセスを許可する] で、Kaspersky Endpoint Security の Web プラグインを選択し、[OK] をクリックします。
8. [回復キーを取得] をクリックします。
現在のダイアログウインドウに回復キーが表示されます。
9. 任意の方法で回復キーを保存します。

クライアントコンピュータでこの回復キーを使用し、暗号化されたドライブにアクセスします。

[インストール種別] ウインドウ

[すべて表示](#) | [すべて隠す](#)

[インストールするパッケージ] セクションでは、クライアントコンピュータにインストールするコンポーネントを選択できます。

[スキャン](#)

このチェックボックスで、Kaspersky Endpoint Security のインストールパッケージにスキャンのコンポーネントを追加します。

このチェックボックスは既定でオンになっており、オフにできません。

ファイル脅威対策

Kaspersky Endpoint Security のインストールパッケージに、ファイル脅威対策のコンポーネントを追加するかどうかを選択します。

このチェックボックスをオンにすると、Kaspersky Endpoint Security のインストールパッケージにファイル脅威対策のコンポーネントが追加されます。

このチェックボックスをオフにすると、ファイル脅威対策のコンポーネントが Kaspersky Endpoint Security インストールパッケージに含まれません。

既定では、このチェックボックスはオンです。

ウェブ脅威対策

Kaspersky Endpoint Security のインストールパッケージに、ウェブ脅威対策のコンポーネントを追加するかどうかを選択します。

このチェックボックスをオンにすると、Kaspersky Endpoint Security のインストールパッケージにウェブ脅威対策のコンポーネントが追加されます。

このチェックボックスをオフにすると、ウェブ脅威対策のコンポーネントが Kaspersky Endpoint Security インストールパッケージに含まれません。

既定では、このチェックボックスはオンです。

ネットワーク脅威対策

Kaspersky Endpoint Security のインストールパッケージに、ネットワーク脅威対策のコンポーネントを追加するかどうかを選択します。

このチェックボックスをオンにすると、Kaspersky Endpoint Security のインストールパッケージにネットワーク脅威対策のコンポーネントが追加されます。

このチェックボックスをオフにすると、ネットワーク脅威対策のコンポーネントが Kaspersky Endpoint Security インストールパッケージに含まれません。

既定では、このチェックボックスはオンです。

ネットワークエージェントコネクタ

このチェックボックスで、Kaspersky Endpoint Security のインストールパッケージにネットワークエージェントコネクタのコンポーネントを追加します。

このチェックボックスは既定でオンになっており、オフにできません。

[ライセンス情報] ウィンドウ

[すべて表示](#) | [すべて隠す](#)

[**ライセンス情報**] ウィンドウで、ライセンスの有効期限、このライセンスで本製品を使用可能なコンピュータの台数、ライセンス種別など、ライセンスに関する情報を表示できます。

予備のライセンスとして追加

特定のライセンス情報ファイルやアクティベーションコードを予備のライセンスとして追加するかどうかを設定します。

このチェックボックスをオンにすると、ライセンス情報ファイルまたはアクティベーションコードが予備のライセンスとして追加されます。

このチェックボックスをオフにすると、ライセンス情報ファイルまたはアクティベーションコードが現在のライセンスとして追加されます。

既定では、このチェックボックスはオフです。

[スキャン] ウィンドウ

[すべて表示](#) | [すべて隠す](#)

スキャン範囲

このリンクをクリックすると表示されるウィンドウで、[スキャン範囲を作成できます](#)。

「**悪意のあるオブジェクトが検知された場合**」セクションでは、Kaspersky Endpoint Security が感染したオブジェクトを検知した時に実行する動作を選択できます。

スキャン後に手動選択する

スキャンが完了するまでオブジェクトを処理しません。スキャンが完了すると、感染したオブジェクトの情報の通知が表示され、実行する処理を選択できます。選択できる処理のオプションは、オブジェクトの種別によって異なります。

既定では、このオプションがオンです。

すぐに手動選択する

感染したオブジェクトを検知すると、各オブジェクトの情報の通知が表示され、その後の処理をユーザが選択するように要求されます。選択できる処理のオプションは、オブジェクトの種別によって異なります。

手動選択しない

検知したオブジェクトに関する情報をレポートに記録しますが、処理は行いません。

自動的に駆除

感染したオブジェクトの検知時に、ユーザに確認を要求せずに駆除するかどうかを選択します。

このチェックボックスをオンにすると、感染したオブジェクトが自動的に駆除されます。

このチェックボックスをオフにすると、感染したオブジェクトがスキップされます。

このチェックボックスは、「手動選択しない」がオンになっている場合に使用可能になります。

既定では、このチェックボックスはオンです。

駆除、駆除できない場合は削除

感染した、または感染の可能性があるオブジェクトが駆除できない場合に自動的に削除するかどうかを選択します。

このチェックボックスをオンにすると、感染したオブジェクトが駆除できなかった場合に、そのオブジェクトを削除します。

このチェックボックスをオフにすると、感染したオブジェクトが駆除できなかった場合に、そのオブジェクトを削除しません。

このチェックボックスは、「手動選択しない」と「自動的に駆除」がオンになっている場合に表示されます。

既定では、このチェックボックスはオンです。

「**ファイル種別**」セクションでは、Kaspersky Endpoint Security でスキャンするファイルの形式を選択できます。

すべてのファイルをスキャン

実行中のファイルシステムオブジェクト、開いているファイルシステムオブジェクト、保存されたファイルシステムオブジェクトをすべてスキャンします。

アプリケーションとドキュメントをスキャン（内容で判断）

感染の可能性があるオブジェクトのみをファイル形式に基づいてスキャンします。

ファイル形式のリストはカスペルスキーが定義し、Kaspersky Endpoint Security の定義データベースに含まれます。

アプリケーションとドキュメントをスキャン（拡張子で判断）

感染の可能性があるオブジェクトのみをファイルの拡張子に基づいてスキャンします。

ファイルの拡張子のリストはカスペルスキーが定義し、Kaspersky Endpoint Security の定義データベースに含まれます。

拡張子なしのファイルは常時スキャンされます。

「**最適化**」セクションでは、スキャンのパフォーマンスを設定できます。

新しいファイルと変更されたファイルのみスキャンする

このチェックボックスは、新しいファイルまたは前回のスキャン以降に変更されたファイルとして認識したこれらのファイルのみのスキャンを有効または無効にします。

このチェックボックスをオンにすると、新しいファイルまたは前回のスキャン以降に変更されたファイルであると認識されたファイルのみをスキャンします。

このチェックボックスをオフにすると、すべてのファイルをスキャンします。

読み取り専用システムボリュームのスキャンをスキップする

読み取り専用のシステムボリュームのスキャンをスキャンするかどうかを選択します。

このチェックボックスをオンにすると、読み取り専用のシステムボリュームのスキャンがスキップされ、スキャンにかかる時間が大幅に短縮されます。

このチェックボックスをオフにすると、読み取り専用のシステムボリュームをスキャンします。

既定では、このチェックボックスはオンです。

次のサイズより大きいファイルのスキャンをスキップする

指定のサイズを超えるファイルをスキャンから除外するかどうかを選択します。

このチェックボックスをオンにすると、指定のサイズを超えるファイルをスキップします。

このチェックボックスをオフにすると、ファイルサイズに関係なくファイルをスキャンします。

既定では、このチェックボックスはオフです。

既定では、サイズは 100 MB に設定されています。

スキャン時間が次を超えたファイルをスキップする

ファイルのスキャンの制限時間を設定するかどうかを選択します。ファイルのスキャンが指定した時間を超えた場合、そのファイルをスキップします。

このチェックボックスをオンにすると、ファイルのスキャンが指定した時間を超えた場合、そのファイルをスキップします。

このチェックボックスをオフにすると、スキャンの時間に関係なくファイルをスキャンします。

既定値は 30 秒です。

「**複合ファイル**」セクションでは、スキャンする複合ファイルの種別を選択できます。

圧縮ファイルをスキャンする

圧縮ファイルのスキャンを有効または無効にします。

このチェックボックスをオンにすると、圧縮ファイルをスキャンします。

このチェックボックスをオフにすると、スキャン中に圧縮ファイルをスキップします。

すべて

Kaspersky Endpoint Security は、すべての圧縮ファイルをスキャンします。

このオプションは、「**圧縮ファイルをスキャンする**」がオンになっている場合に使用可能になります。

新規のみ

Kaspersky Endpoint Security は、新規の圧縮ファイルのみをスキャンします。

このオプションは、「**圧縮ファイルをスキャンする**」がオンになっている場合に使用可能になります。

パスワードで保護された圧縮ファイルをスキャンする

パスワードで保護された圧縮ファイルのスキャンを有効または無効にします。

このチェックボックスをオンにすると、パスワード保護された圧縮ファイルをスキャンします。

このチェックボックスをオフにすると、スキャン中にパスワード保護された圧縮ファイルをスキップします。

OLE 埋め込みオブジェクトをスキャンする

Excel スプレッドシート、マクロ、メールの添付ファイルなど、ファイルに埋め込まれたオブジェクトをスキャンするかどうかを選択します。

このチェックボックスをオンにすると、埋め込み OLE オブジェクトをスキャンします。

このチェックボックスをオフにすると、スキャン中に埋め込み OLE オブジェクトをスキップします。

すべて

Kaspersky Endpoint Security は、すべての OLE オブジェクトをスキャンします。
このオプションは、[OLE 埋め込みオブジェクトをスキャンする] がオンになっている場合に選択できます。

新規のみ

Kaspersky Endpoint Security は、新規の OLE 埋め込みオブジェクトのみをスキャンします。
このオプションは、[OLE 埋め込みオブジェクトをスキャンする] がオンになっている場合に選択できます。

メール形式のファイルをスキャンする

メール形式のファイルとメールデータベースをスキャンするかどうかを選択します。
このチェックボックスをオンにすると、メール形式のファイルとメールデータベースをスキャンします。
このチェックボックスをオフにすると、スキャン中にメール形式のファイルとメールデータベースをスキップします。

[スキャン範囲] ウィンドウ

[すべて表示](#) | [すべて隠す](#)

追加

クリックすると ダイアログが開き、スキャン範囲に追加するファイルやフォルダ、ファイルのマスクまたはフォルダのマスクを指定できます。

削除

スキャン範囲からオブジェクトを削除します。
このボタンは、オブジェクトの隣のチェックボックスが選択されている場合に使用できます。
既定でスキャン範囲に含まれているオブジェクトは削除できません。

スキャン範囲

マルウェアスキャン中にスキャンされるオブジェクトが表示されます。

ステータス

この列のスイッチで、スキャン範囲に追加されたオブジェクトをスキャンするかどうかを選択できます。
スイッチをオンにすると、Kaspersky Endpoint Security は対応するオブジェクトをスキャンします。
スイッチをオフにすると、Kaspersky Endpoint Security は対応するオブジェクトをスキャンしません。

詳細

この列は、Kaspersky Endpoint Security が対応するオブジェクトのサブフォルダをスキャンするかどうかを示します。

注意：Kaspersky Endpoint Security は、OneDrive や iCloud ストレージ、その他のクラウドストレージにあるファイルをスキャンしません。これらのファイルをスキャン範囲から除外してください。そうしないと、スキャンタスクが「感染したファイルが削除されませんでした」というエラーで終了する可能性があります。

[スキャン範囲を追加] ダイアログ

[すべて表示](#) | [すべて隠す](#)

ファイル名、フォルダ名、またはマスクを入力

ファイルやフォルダのパス、またはファイルやフォルダのマスク。

フォルダ名

オブジェクトをフォルダとしてスキャンするかどうかを選択します。

このチェックボックスをオンにすると、**「ファイル名、フォルダ名、またはマスクを入力」** で指定したオブジェクトをフォルダとしてスキャンします。

このチェックボックスをオフにすると、**「ファイル名、フォルダ名、またはマスクを入力」** で指定したオブジェクトをファイルとしてスキャンします。

既定では、このチェックボックスはオンです。

サブフォルダを含める

このチェックボックスは、**「ファイル名、フォルダ名、またはマスクを入力」** で指定したフォルダのサブフォルダのスキャンを有効または無効にします。

このチェックボックスをオンにすると、マルウェアスキャン中にサブフォルダをスキャンします。

このチェックボックスをオフにすると、**「ファイル名、フォルダ名、またはマスクを入力」** フィールドで指定したフォルダのみをマルウェアスキャン中にスキャンします。

既定では、このチェックボックスはオンです。

注意：Kaspersky Endpoint Security は、OneDrive や iCloud ストレージ、その他のクラウドストレージにあるファイルをスキャンしません。これらのファイルをスキャン範囲から除外してください。そうしないと、スキャンタスクが「感染したファイルが削除されませんでした」というエラーで終了する可能性があります。

ファイルパラメータのウィンドウ

次の種別のファイルハッシュがサポートされています：

- **MD5**

この種類のハッシュは **32** 文字で、**0-9**、**a-f**、**A-F** を含む必要があります。

- **SHA256**

この種類のハッシュは **64** 文字で、**0-9**、**a-f**、**A-F** を含む必要があります。

「ネットワーク」 ウィンドウ

[すべて表示](#) | [すべて隠す](#)

「プロキシサーバ設定」 セクションでは、プロキシサーバの使用とプロキシサーバへの接続に使用する設定を編集できます。

プロキシサーバを使用しない

このオプションをオンにすると、定義データベースとソフトウェアモジュールのアップデート元への接続にプロキシサーバを使用しません。

システムのプロキシサーバ設定を使用する

このオプションをオンにすると、定義データベースとソフトウェアモジュールのアップデート元への接続に、お使いのオペレーティングシステムで指定したプロキシサーバの設定を使用します。

既定では、このオプションがオンです。

指定したプロキシサーバ設定を使用する

このオプションをオンにすると、定義データベースとソフトウェアモジュールのアップデート元への接続に、指定したプロキシサーバの設定を使用します。

アドレス

プロキシサーバの IP アドレスまたは識別名。

このチェックボックスは、**「指定したプロキシサーバ設定を使用する」** をオンにすると使用できます。

ポート

プロキシサーバのポート番号。

既定のポート番号は 8080 です。

このチェックボックスは、**「指定したプロキシサーバ設定を使用する」** をオンにすると使用できます。

認証を使用する

プロキシサーバへの接続時に認証を使用するかどうかを選択します。

このチェックボックスをオンにすると、プロキシサーバへの接続時にユーザの認証情報が要求されます。

このチェックボックスをオフにすると、プロキシサーバへの接続時にユーザの認証情報は要求されません。

既定では、このチェックボックスはオンです。

このチェックボックスは、**「指定したプロキシサーバ設定を使用する」** をオンにすると使用できます。

ユーザ名

プロキシサーバへ接続するためのユーザ名。

この入力フィールドは、**「指定したプロキシサーバ設定を使用する」** と **「認証を使用する」** をオンにすると使用できます。

パスワード

指定したユーザ名のパスワード。

この入力フィールドは、**「指定したプロキシサーバ設定を使用する」** と **「認証を使用する」** をオンにすると使用できます。

表示

このボタンをクリックすると、**「パスワード」** フィールドに入力したパスワードが表示されます。

ローカルアドレスにはプロキシサーバを使用しない

ローカルまたはネットワークフォルダからの定義データベースとソフトウェアモジュールのアップデートに、プロキシサーバを使用するかどうかを選択します。

このチェックボックスをオンにすると、ローカルまたはネットワークフォルダからの定義データベースとソフトウェアモジュールのアップデートに、プロキシサーバを使用しません。

このチェックボックスをオフにすると、ローカルまたはネットワークフォルダからの定義データベースとソフトウェアモジュールのアップデートに、プロキシサーバを使用します。

既定では、このチェックボックスはオンです。

このチェックボックスは、**「指定したプロキシサーバ設定を使用する」** をオンにすると使用できます。

「セキュアな接続をチェック」 セクションで、Kaspersky Endpoint Security がセキュアな接続 (HTTPS) をスキャンするかどうかを指定できます。

セキュアな接続 (HTTPS) のチェック

「セキュアな接続 (HTTPS) をチェック」 スイッチで、HTTPS プロトコルを使用して確立された安全な接続をスキャンし、危険な Web サイトへのユーザのアクセスをウェブコントロールがブロックした時に通知を表示するかどうかを設定します。

「セキュアな接続 (HTTPS) をチェック」 スイッチをオンにすると、Kaspersky Endpoint Security は次の動作を行います：

- Safari、Google Chrome、または Firefox で、HTTPS プロトコルを使用してコンピュータで送受信するデータを、ウェブ脅威対策がスキャンします。
- 危険な Web サイトへのユーザのアクセスをウェブコントロールがブロックした時、クライアントコンピュータ上に通知を表示します。

「セキュアな接続 (HTTPS) をチェック」 スイッチをオフにすると、Kaspersky Endpoint Security は次の動作を行います：

- HTTPS プロトコルを使用してコンピュータが送受信するデータを、ウェブ脅威対策はスキャンしません。
- 危険な Web サイトへのユーザのアクセスをウェブコントロールがブロックした時、クライアントコンピュータ上に通知を表示しません。

このスイッチは既定ではオンになっています。

Firefox が使用する証明書ストアを選択セクションでは、Mozilla Firefox ブラウザで暗号化された HTTPS トラフィックをチェックするための証明書ストアを選択できます。

[システムルートキーチェーン（推奨）](#)

このオプションをオンにすると、Kaspersky Endpoint Security はシステムルートキーチェーンのルート証明書を使用して、Mozilla Firefox ブラウザで暗号化された HTTPS トラフィックをチェックします。

既定では、このオプションがオンです。

[Mozilla Firefox のブラウザー設定の証明書ストア](#)

このオプションをオンにすると、Kaspersky Endpoint Security はブラウザの証明書ストアからの証明書を使用します。

この場合、Kaspersky Endpoint Security 証明書を Mozilla Firefox ブラウザの証明書ストアに手動で追加する必要があります。詳細は、「[カスタム証明書](#)」を [Mozilla Firefox 証明書ストアに追加する方法](#)」を参照してください。

「**信頼済みルート証明書**」セクションで、信頼済みルート証明書のリスを管理できます。

[信頼済みルート証明書を管理](#)

このリンクをクリックすると、対応するサーバに通知なしで接続する [信頼済みルート証明書のリストを作成するウィンドウ](#)が表示されます。

「**監視対象ポート**」セクションでは、Kaspersky Endpoint Security で監視するポートを設定できます。

[選択したポート](#)

このリンクをクリックすると [ウィンドウが開き、Kaspersky Endpoint Security で監視するポートのリストを設定できます。](#)

[強制適用](#)

「**強制適用**」スイッチをオンにすると、Kaspersky Endpoint Security は、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値の変更を禁止します。

「**強制適用**」スイッチをオフにすると、Kaspersky Endpoint Security では、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値が変更できます。

「信頼済みルート証明書を管理」 ウィンドウ

[すべて表示](#) | [すべて隠す](#)

[追加](#)

このボタンをクリックすると、信頼済みと判断される証明書を追加するダイアログが表示されます。

[削除](#)

このボタンをクリックすると、選択した証明書が信頼する証明書のリストから削除されます。

[信頼済み証明書のリスト](#)

信頼済みルート証明書の名前を表示するリスト。

既定では、リストは空白になっています。

[強制適用](#)

「**強制適用**」スイッチをオンにすると、Kaspersky Endpoint Security は、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値の変更を禁止します。

「**強制適用**」スイッチをオフにすると、Kaspersky Endpoint Security では、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値が変更できます。

[監視対象ポート] ウィンドウ

[すべて表示](#) | [すべて隠す](#)

監視対象ポートのリスト

送信データの監視を設定できるポートのリスト。

既定では、ポートのリストには、最も一般的なサービスで頻繁に使用されるポートが表示されています。

追加

このボタンをクリックすると [ダイアログが開き、監視対象にするポートを追加できます](#)。

削除

このボタンをクリックすると、選択したポートがリストから削除されます。

このボタンは、ポートの隣のチェックボックスが選択されている場合に使用できます。

ポート

この列には、ポート番号が表示されます。

ステータス

この列には、ポートを介して送信されるデータの監視ステータスを示すスイッチが表示されます。

ステータスが「[監視されています](#)」の場合、対応するポートを介して送信されるトラフィックは、Kaspersky Endpoint Security によってスキャンされます。

ステータスが「[監視されていません](#)」の場合、対応するポートを介して送信されるトラフィックは、Kaspersky Endpoint Security によってスキャンされません。

説明

この列には、ポートの説明が表示されます。

[ポートの追加] ダイアログ

[すべて表示](#) | [すべて隠す](#)

ポートの入力フィールド

送信データをスキャンするポートの番号。

説明の入力フィールド

ポートの種別など、ポートに関する追加情報。

[信頼ゾーン] ウィンドウの [ファイルとフォルダ] セクション

[すべて表示](#) | [すべて隠す](#)

追加

このボタンをクリックすると、[信頼ゾーンにファイルまたはフォルダを追加するダイアログ](#)が開きます。

削除

クリックすると、除外対象のリストから選択されたファイルまたはフォルダを削除します。

このボタンは、ファイルまたはフォルダの隣のチェックボックスが選択されている場合に使用できます。

ファイルまたはフォルダ

この列には、信頼ゾーンに追加されたファイルまたはフォルダが含まれます。

ステータス

この列のスイッチで、信頼ゾーンに追加されたファイルまたはフォルダをスキャンするかどうかを選択できます。
スイッチをオンにすると、Kaspersky Endpoint Securityは対応するファイルまたはフォルダをスキャンしません。
スイッチがオフになっている場合、Kaspersky Endpoint Securityは対応するファイルまたはフォルダをスキャンします。

コメント

信頼ゾーンに追加されたファイルまたはフォルダに関する情報です。

強制適用

〔強制適用〕スイッチをオンにすると、Kaspersky Endpoint Security は、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値の変更を禁止します。
〔強制適用〕スイッチをオフにすると、Kaspersky Endpoint Securityでは、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値が変更できます。

〔除外を追加〕 ダイアログ

[すべて表示](#) | [すべて隠す](#)

ファイル名、フォルダ名、またはマスクを入力の入力フィールド

保護範囲から除外するファイル、フォルダ、ファイルまたはフォルダのマスクのパス。

サブフォルダを含める

〔ファイル名、フォルダ名、またはマスクを入力〕で指定したフォルダのサブフォルダをスキャンするかどうかを選択します。
このチェックボックスをオンにすると、マルウェアスキャン中、指定したフォルダのサブフォルダはスキャンされません。
このチェックボックスをオフにすると、〔ファイル名、フォルダ名、またはマスクを入力〕で指定したフォルダのみがスキャンされなくなります。指定したフォルダのサブフォルダはスキャンされます。
既定では、このチェックボックスはオンです。

〔コンポーネント〕セクションでは、指定されたファイルまたはフォルダをスキャンしないコンポーネントを選択できます。

すべて

スキャンコンポーネントもファイル脅威対策コンポーネントも、指定されたファイルまたはフォルダをスキャンしません。

リストから選択

このオプションを使用すると、コンポーネントを選択できます。

ファイル脅威対策

このチェックボックスをオンにすると、ファイル脅威対策コンポーネントは指定されたファイルまたはフォルダをスキャンしません。
このチェックボックスは、〔リストから選択〕をオンにすると使用可能になります。

スキャン

このチェックボックスをオンにすると、スキャンコンポーネントは指定されたファイルまたはフォルダをスキャンしません。
このチェックボックスは、〔リストから選択〕をオンにすると使用可能になります。

コメントの入力フィールド

信頼ゾーンに追加されたファイルまたはフォルダに関する情報です。

「**ステータス**」セクションでは、除外をアクティブにするかどうかを選択できます。

無効

Kaspersky Endpoint Securityは対応するファイルまたはフォルダをスキャンします。

有効

Kaspersky Endpoint Securityは対応するファイルまたはフォルダをスキャンしません。

「信頼ゾーン」 ウィンドウの 「信頼済みアプリケーション」 セクション

[すべて表示](#) | [すべて隠す](#)

信頼済みアプリケーションのリスト

ネットワーク活動が Kaspersky Endpoint Security によって監視されない信頼済みアプリケーションのリストです。

追加

このボタンをクリックすると [ダイアログが開き、ネットワーク活動が監視されないアプリケーションへのパスを入力できます](#)。

削除

このボタンをクリックすると、選択した信頼済みアプリケーションがリストから削除されます。
このボタンは、信頼済みアプリケーションの隣のチェックボックスが選択されている場合に使用できます。

アプリケーション

この列には、アプリケーション名またはアプリケーションへのパスの最後のセグメントが含まれます。

ステータス

この列には、アプリケーションネットワーク活動の監視ステータスを示すスイッチが含まれています。
ステータスが「**有効**」な場合、対応するアプリケーションのネットワーク活動は Kaspersky Endpoint Security によって監視されません。
ステータスが「**無効**」な場合、対応するアプリケーションのネットワーク活動は Kaspersky Endpoint Security によって監視されます。

パス

この列には、クライアントコンピュータ上の手動で追加するアプリケーションのパスが表示されます。

強制適用

「**強制適用**」スイッチをオンにすると、Kaspersky Endpoint Security は、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値の変更を禁止します。
「**強制適用**」スイッチをオフにすると、Kaspersky Endpoint Security では、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値が変更できます。

「アプリケーションの追加」 ダイアログ

[すべて表示](#) | [すべて隠す](#)

パスの入力フィールド

ネットワーク活動やファイル操作が監視されないアプリケーションへのパス。

コード署名の要件 [?](#)

Kaspersky Endpoint Security によって活動が監視されないアプリケーションのコード署名の要件。

これはオプションのパラメータです。

オプション [?](#)

このセクションでは、Kaspersky Endpoint Security で監視しない活動の種類を選択できます。

ファイル操作を監視しない [?](#)

クライアントコンピュータ上のファイルを使用したアプリケーションの動作の監視を有効または無効にします。

このチェックボックスをオンにすると、アプリケーションのファイルの動作は監視されません。

このチェックボックスをオフにすると、アプリケーションのファイルの動作を監視します。

既定では、このチェックボックスはオンです。

ネットワーク活動を監視しない [?](#)

クライアントコンピュータ上のアプリケーションが送受信するインターネットトラフィックの監視を有効または無効にします。

このチェックボックスをオンにすると、アプリケーションのネットワーク活動は監視されません。

このチェックボックスをオフにすると、アプリケーションのネットワーク活動を監視します。

既定では、このチェックボックスはオンです。

[詳細設定] セクション

[すべて表示](#) | [すべて隠す](#)

プロテクション [?](#)

このリンクをクリックすると、[\[プロテクション\]](#) ウィンドウが開き、ユーザのコンピュータにインストールされている Kaspersky Endpoint Security の全般設定を管理し、Kaspersky Endpoint Security が検知するオブジェクト種別を選択できます。

レポートとバックアップ [?](#)

このリンクをクリックすると、[\[レポートとバックアップ\]](#) ウィンドウが開き、レポートとバックアップの設定を管理できます。

ユーザインターフェイス [?](#)

このリンクをクリックすると、[\[ユーザインターフェイス\]](#) ウィンドウが開き、Kaspersky Endpoint Security で表示される通知、Kaspersky Security Center で表示されるイベントの表示言語、Kaspersky Endpoint Security の追加設定を設定できます。

ネットワーク [?](#)

このリンクをクリックすると、[\[ネットワーク\]](#) ウィンドウが開き、プロキシサーバの設定を管理したり、暗号化された接続 (HTTPS) のスキャンを有効または無効にしたり、Mozilla Firefox ブラウザで暗号化された HTTPS トラフィックをチェックするための証明書ストアを選択したり、監視対象ポートを設定したりできます。

信頼ゾーン [?](#)

このリンクをクリックすると、[\[信頼ゾーン\]](#) ウィンドウが開き、ファイル脅威対策やスキャンタスクの除外を追加したり、信頼するアプリケーションを設定したりできます。

[プロテクション] ウィンドウ

[すべて表示](#) | [すべて隠す](#)

[全般] セクションでは、リモートコンピュータのプロテクションを有効または無効に設定したり、コンピュータの電源を入れた時またはオペレーティングシステムを再起動した時に本製品が自動的に起動するよう設定できます。

コンピュータ起動時に本製品を起動する

リモートコンピュータの電源を入れた時、またはオペレーティングシステムが再起動した時に本製品が自動的に起動するかどうかを設定します。

このチェックボックスをオンにすると、リモートコンピュータの電源を入れた時、またはオペレーティングシステムが再起動した時に Kaspersky Endpoint Security が自動的に起動します。

このチェックボックスをオフにすると、リモートコンピュータの電源を入れた時、またはオペレーティングシステムが再起動した時に Kaspersky Endpoint Security が自動的に起動しません。

既定では、このチェックボックスはオンです。

重要：Kaspersky Endpoint Security が実行されていないときにこのチェックボックスをオンにすると、変更はローカルで本製品を開始するか、Kaspersky Security Center を使用して本製品を開始した後にのみ適用されます。

保護機能を有効にする

Kaspersky Endpoint Security がインストールされているリモートコンピュータの保護機能を有効または無効にします。

このチェックボックスをオンにすると、リモートコンピュータの保護機能が有効になります。

このチェックボックスをオフにすると、リモートコンピュータの保護機能が無効になります。

既定では、このチェックボックスはオンです。

「**検知するオブジェクトの種別**」セクションで、Kaspersky Endpoint Security で検知するオブジェクトの種別を選択できます。

ウイルス、ワーム、トロイの木馬、悪意のあるツール、アドウェア、オートダイアラー

次の種別のプログラムを検知するかどうかを設定します：

- すべての種別のマルウェア。
- コンピュータで広告（バナーなど）を表示したり、Web ブラウザでの検索結果を Web サイトの広告に置き換えたりするアプリケーション。
- 利用者の許可なくコンピュータのモデムによる電話回線接続を確立するアプリケーション。

このチェックボックスは既定でオンになっており、オフにできません。

ユーザに損害を与える目的で悪用される可能性がある正規のソフトウェア

悪意がなく危険でもないが、特定の状況下でコンピュータに損害を与える目的で悪用される可能性があるアプリケーションを検知するかどうかを選択します。

このチェックボックスをオンにすると、コンピュータまたは個人データに損害を与える可能性がある正規のソフトウェアが検知されます。

このチェックボックスをオフにすると、コンピュータまたは個人データに損害を与える目的で悪用される可能性がある正規のソフトウェアが検知されません。

既定では、このチェックボックスはオフです。

「**詳細**」セクションでは、省電力モードを有効または無効にできます。

バッテリー使用中はスケジュールされたタスクをスキップする

バッテリー電源で動作しているコンピュータで、スケジュールされているスキャンタスクを起動するかどうかを選択します。

このチェックボックスをオンにすると、バッテリー電源で動作しているコンピュータではスケジュールされているスキャンタスクを起動しません。

このチェックボックスをオフにすると、バッテリー電源で動作しているコンピュータでもスケジュールされているスキャンタスクを起動します。

既定では、このチェックボックスはオンです。

スキャンタスクによる CPU の使用を制限する

オンデマンドスキャンタスクの保護対象デバイスの CPU 使用率は、対応する入力フィールドで指定された値に制限されます。

このオプションをオンにすると、Kaspersky Endpoint Security のパフォーマンスが低下する可能性があります。

既定では、このオプションはオフです。

上限（パーセント）

Kaspersky Endpoint Security によるスキャンタスクの使用可能な最大 CPU 使用率。

このフィールドは、「スキャンタスクによる CPU の使用を制限する」がオンになっている場合に限り使用できます。

注意：この制限は、すべての CPU コアからの累積に対して適用されます。アクティビティモニタに表示される CPU 使用率は、各 CPU コアの使用率の合計であり、そのため、100 % を超えた数値が表示される場合があります。

強制適用

「強制適用」スイッチをオンにすると、Kaspersky Endpoint Security は、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値の変更を禁止します。

「強制適用」スイッチをオフにすると、Kaspersky Endpoint Security では、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値が変更できます。

「レポートとバックアップ」 ウィンドウ

[すべて表示](#) | [すべて隠す](#)

「レポート」セクションでは、Kaspersky Endpoint Security の実行中に発生するイベントのレポートの生成および保存に関する設定を編集できます。

レポートを削除するまでの期間

指定された期間経過後にレポートを削除するかどうかを選択します。

このチェックボックスをオンにすると、指定された期間の経過後にレポートが削除されます。既定では、レポートは 30 日間保存されます。

このチェックボックスをオフにすると、レポートを無期限で保存します。

既定では、このチェックボックスはオンです。

緊急イベント以外も記録する

緊急イベント以外のイベント（情報イベントなど）をレポートへ記録するかどうかを選択します。緊急イベント以外は、セキュリティに影響を与えません。

このチェックボックスをオンにすると、レポートに情報イベントを記録します。

このチェックボックスをオフにすると、レポートに情報イベントを記録しません。

既定では、このチェックボックスはオフです。

最近のイベントのみを保存する

前回タスクを実行した際の重要なイベントに関する情報のみを保存するかどうかを選択します。

このチェックボックスをオンにすると、前回のタスク実行時の緊急イベント以外のイベントの情報が、タスクの開始時に毎回削除されます。ただし、重要な情報（検知したマルウェアの情報など）は、レポートに保持されます。

このチェックボックスをオフにすると、前回のタスクの実行時のイベントはすべて保持されます。

既定では、このチェックボックスはオフです。

「バックアップ」セクションでは、バックアップにオブジェクトを保存する期間を指定できます。

オブジェクトを削除するまでの期間

指定した期間の経過後に、バックアップからオブジェクトを削除するかどうかを選択します。

このチェックボックスをオンにすると、指定された期間が過ぎるとオブジェクトがバックアップから削除されます。既定の保存期間は **30 日** です。

このチェックボックスをオフにすると、オブジェクトがバックアップに無期限に保存されます。

既定では、このチェックボックスはオンです。

強制適用

〔**強制適用**〕スイッチをオンにすると、Kaspersky Endpoint Security は、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値の変更を禁止します。

〔**強制適用**〕スイッチをオフにすると、Kaspersky Endpoint Security では、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値が変更できます。

〔ユーザーインターフェイス〕 ウィンドウ

[すべて表示](#) | [すべて隠す](#)

〔**製品インターフェイス**〕セクションでは、リモートコンピュータのメニューバーにある製品アイコンの表示の設定およびユーザーが Kaspersky Endpoint Security のメインウィンドウを開いてインターフェイスを使用するかどうかを設定できます。

製品アイコンをメニューバーに表示する

リモートコンピュータのメニューバーに製品アイコンを表示するかどうかを選択します。

このチェックボックスをオンにすると、製品アイコンがメニューバーに表示されます。

このチェックボックスをオフにすると、製品アイコンがメニューバーに表示されません。

既定では、このチェックボックスはオンです。

ユーザーに製品の表示を許可する

このチェックボックスでは、ユーザーがリモートコンピュータから Kaspersky Endpoint Security のメインウィンドウを表示してインターフェイスを使用するかどうかを選択します。

このチェックボックスをオンにすると、ユーザーはリモートコンピュータから Kaspersky Endpoint Security のメインウィンドウを表示してインターフェイスを使用できます。

このチェックボックスをオフにすると、ユーザーはリモートコンピュータからメインウィンドウを開くことはできず、インターフェイスは表示されません。

既定では、このチェックボックスはオンです。

〔**通知**〕セクションでは、Kaspersky Endpoint Security のイベントの通知を有効にして、通知の種別を選択できます。

通知

〔**通知**〕スイッチで、Kaspersky Endpoint Security のイベントを通知するかどうかを選択します。

〔**通知**〕スイッチをオンにすると、Kaspersky Endpoint Security のコンポーネントの実行中に発生するイベントについて、通知が表示されます。

〔**通知**〕スイッチをオフにすると、Kaspersky Endpoint Security のコンポーネントの実行中に発生するイベントについて、通知は表示されません。

このスイッチは既定ではオンになっています。

ユーザー通知

このリンクをクリックすると [ウィンドウが開き、すべての種別のイベントで使用する通知の種別を選択できます](#)。

〔**ユーザーに本製品の終了を許可**〕セクションでは、リモートコンピュータのユーザーに Kaspersky Endpoint Security を終了する権限を付与するかどうかを設定できます。

製品アイコンのコンテキストメニューに「終了」を表示する

メニューバーに表示される製品アイコンのコンテキストメニューに **「終了」** の項目を表示するかどうかを選択します。

このチェックボックスをオンにすると、**「終了」** の項目は製品アイコンのコンテキストメニューで使用できます。リモートコンピュータのユーザは、使用しているコンピュータの **Kaspersky Endpoint Security** を終了できるようになります。

このチェックボックスをオフにすると、**「終了」** の項目は製品アイコンのコンテキストメニューで使用できなくなります。リモートコンピュータのユーザは、使用しているコンピュータの **Kaspersky Endpoint Security** を終了できません。

既定では、このチェックボックスはオンです。

「Kaspersky Security Center でのイベント」 セクションでは、Kaspersky Security Center での Kaspersky Endpoint Security のイベントの表示言語を選択できます。

表示言語

このドロップダウンリストから、Kaspersky Security Center での Kaspersky Endpoint Security のイベントの表示言語を選択できます。

「制限」 セクションでは、リモートコンピュータの Kaspersky Endpoint Security のライセンスとアップデートをローカルで管理する権限を付与できます。

ユーザにデバイス上でのアップデートの管理を許可

リモートコンピュータの Kaspersky Endpoint Security のアップデートを、ローカルで管理できるようにするかどうかを選択します。

このチェックボックスをオンにすると、リモートコンピュータの Kaspersky Endpoint Security のアップデートをローカルで管理できます。

このチェックボックスをオフにすると、リモートコンピュータの Kaspersky Endpoint Security のアップデートは、Kaspersky Security Center の Kaspersky Endpoint Security 管理プラグインを使用しないと管理できません。

既定では、このチェックボックスはオンです。

ユーザにデバイス上でのライセンスの管理を許可

リモートコンピュータの Kaspersky Endpoint Security のライセンスを、ローカルで管理できるようにするかどうかを選択します。

このチェックボックスをオンにすると、リモートコンピュータの Kaspersky Endpoint Security のライセンスをローカルで管理できます。

このチェックボックスをオフにすると、リモートコンピュータの Kaspersky Endpoint Security のアップデートは、Kaspersky Security Center の Kaspersky Endpoint Security 管理プラグインを使用しないと管理できません。

既定では、このチェックボックスはオンです。

「パスワードによる保護」 セクションでは、パスワードを設定および変更して、ユーザのデバイスでの不要な操作を制限できます。

パスワードによる保護

「パスワードによる保護」 スイッチは、ユーザのデバイス上での不要な操作に対するパスワードによる保護を有効または無効にします。

「パスワードによる保護」 スイッチをオンにすると、パスワードを設定し、デバイス上でのユーザの操作を制限できます。

「パスワードによる保護」 スイッチをオフにすると、ユーザはパスワードを入力せずに不要な操作を実行できます。

このスイッチは既定ではオフになっています。

このスイッチをオンにすると、[ユーザのデバイス上での不要な操作を制限するためのパスワードを設定するウィンドウ](#)が開きます。

設定

このボタンをクリックすると、[ユーザのデバイス上での不要な操作を制限するためのパスワードを設定するウィンドウ](#)が開きます。

強制適用

「強制適用」 スイッチをオンにすると、Kaspersky Endpoint Security は、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値の変更を禁止します。

[強制適用] スイッチをオフにすると、Kaspersky Endpoint Securityでは、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値が変更できます。

[ユーザ通知] ウインドウ

[すべて表示](#) | [すべて隠す](#)

イベント

Kaspersky Endpoint Security の実行中に発生する可能性があるイベントのリスト。発生するイベントは次の通りです：

- **緊急イベント**：セキュリティの観点から非常に重要なイベント。
- **機能エラー**：システムの停止を引き起こすイベント。
- **重要なイベント**：ユーザが注意を向けるべきイベント。
- **情報イベント**：実質的に情報のイベント。

通知

バルーンは、ユーザにイベントを通知するポップアップ形式のメッセージです。

[通知] 列のチェックボックスで、特定のカテゴリのイベントに関するポップアップ通知を有効または無効にできます。

サウンド

イベントと関連付けられた通知音。

[サウンド] 列のチェックボックスで、特定のカテゴリのイベントに対する通知音を有効または無効にできます。

[アップデート] セクション

[すべて表示](#) | [すべて隠す](#)

ソフトウェアモジュールをアップデートする

ソフトウェアモジュールをアップデートするかどうかを選択します。定義データベースは常にアップデートされます。

このチェックボックスをオンにすると、ソフトウェアモジュールがアップデートされます。

このチェックボックスをオフにすると、ソフトウェアモジュールはアップデートされません。

既定では、このチェックボックスはオンです。

アップデート元

このリストには定義データベースとソフトウェアモジュールのアップデートをダウンロードしてインストールする、アップデート元のアドレスが表示されます。ローカルフォルダやネットワークフォルダ、FTP サーバ、HTTP サーバをアップデート元として指定できます。

既定では、アップデート元のリストにはカスペルスキーのアップデートサーバーが含まれています。

Kaspersky Security Center Web コンソールで Kaspersky Endpoint Security を管理している場合、アップデート元のリストには既定で Kaspersky Security Center サーバーが含まれています。

Kaspersky Security Center Cloud コンソールを通して Kaspersky Endpoint Security を管理している場合、アップデート元のリストには既定でディストリビューションポイントが含まれています。ディストリビューションポイントの詳細は、[Kaspersky Security Center のヘルプ !\[\]\(11c5349c42fa55c4c7fb0461dfba2a6e_img.jpg\)](#) を参照してください。

リストから既定のアップデート元を削除することはできません。

追加

このボタンをクリックすると表示されるダイアログで、[アップデート元のリストに追加するローカルフォルダやネットワークフォルダのパスや、URL を指定できます。](#)

削除

このボタンをクリックすると、選択したアップデート元がリストから削除されます。
このボタンは、アップデート元に隣接するチェックボックスがオンにされている場合に使用できます。

アップデート元

この列には、Kaspersky Endpoint Security のアップデート元が表示されます。

ステータス

この列のスイッチがオンになっていると、Kaspersky Endpoint Security は、[アップデート元] 列の対応するアップデート元を使用してアップデートを受信します。

この列のスイッチがオフになっていると、Kaspersky Endpoint Security は、[アップデート元] 列の対応するアップデート元を使用してアップデートを受信しません。

強制適用

[強制適用] スイッチをオンにすると、Kaspersky Endpoint Security は、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値の変更を禁止します。

[強制適用] スイッチをオフにすると、Kaspersky Endpoint Security では、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値が変更できます。

[アップデート元を追加] ダイアログ

[すべて表示](#) | [すべて隠す](#)

入力フィールドにローカルまたはネットワークフォルダへのパス、または URL を入力

コピーするアップデートが置かれているアップデート元のアドレス。

ローカルまたはネットワークフォルダのパス、FTP サーバや HTTP サーバの URL や IP アドレスをアップデート元のアドレスとして指定できます。

FTP サーバの URL は、「ftp://<ユーザ名>:<パスワード>@<ホスト>:<ポート>」の形式で指定できます。

[ステータス] セクションで、Kaspersky Endpoint Security が指定された URL をアップデート元として使用するかどうかを指定できます。

無効

URL はアップデート元のリストに追加されますが、Kaspersky Endpoint Security は、この URL をアップデート元として使用しません。

有効

URL がアップデート元のリストに追加され、Kaspersky Endpoint Security は、この URL をアップデート元として使用します。

[データ暗号化] セクション

[すべて表示](#) | [すべて隠す](#)

FileVault ディスク暗号化

[FileVault ディスク暗号化] スイッチで、FileVault ディスク暗号化の管理を有効または無効にします。

[FileVault ディスク暗号化] スイッチをオンにすると、FileVault ディスク暗号化は Kaspersky Security Center からクライアントコンピュータに適用されます。

[FileVault ディスク暗号化] スイッチをオフにすると、FileVault ディスク暗号化は Kaspersky Security Center からクライアントコンピュータに適用されません。

このスイッチは既定ではオフになっています。

注意：[FileVault ディスク暗号化] のスイッチをオフにすると、管理者権限を持つユーザはシステム設定から Mac の起動ディスクを暗号化および復号化できます。FileVault の詳細は、Apple のガイドを参照してください。

ディスクを暗号化する

ポリシーを適用するクライアントコンピュータ上に、アカウント認証情報を入力する要求を表示します。認証情報を入力すると、ユーザの起動ディスクの暗号化が開始されます。

「FileVault ディスク暗号化」スイッチをオンにし、「ディスクを暗号化する」をオンにすると、管理者権限を持つユーザがシステム設定から Mac の起動ディスクを復号化することはできません。

ディスクを復号化する

ポリシーを適用するクライアントコンピュータ上に、アカウント認証情報を入力する要求を表示します。認証情報を入力すると、ユーザの起動ディスクの復号化が開始されます。

「FileVault ディスク暗号化」スイッチをオンにし、「ディスクを復号化する」をオンにすると、管理者権限を持つユーザがシステム設定から Mac の起動ディスクを暗号化することはできません。

強制適用

「強制適用」スイッチをオンにすると、Kaspersky Endpoint Security は、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値の変更を禁止します。

「強制適用」スイッチをオフにすると、Kaspersky Endpoint Security では、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値が変更できます。

「Detection and Response」セクション

[すべて表示](#) | [すべて隠す](#)

Managed Detection and Response

このリンクをクリックすると、[Endpoint Detection and Response \(KATA\) 設定を指定できる](#)ウィンドウが表示されます。

Endpoint Detection and Response

このリンクをクリックすると、[Endpoint Detection and Response \(KATA\) 設定を指定できる](#)ウィンドウが表示されます。

Endpoint Detection and Response (KATA)

このリンクをクリックすると、[Endpoint Detection and Response \(KATA\) 設定を指定できる](#)ウィンドウが表示されます。

「Managed Detection and Response」ウィンドウ

[すべて表示](#) | [すべて隠す](#)

Managed Detection and Response

「Managed Detection and Response」のスイッチで、Kaspersky Managed Detection and Response サービスと対話する Managed Detection and Response コンポーネントを有効または無効に設定できます。このサービスは、組織を標的とするセキュリティ上の脅威を継続的に検知し、排除します。

「Managed Detection and Response」スイッチをオンにして、MDR 設定情報ファイルをインポートすると、コンポーネントが有効になります。

「Managed Detection and Response」スイッチをオフにすると、コンポーネントが無効になります。
このスイッチは既定ではオフになっています。

インポート

このボタンをクリックすると、MDR 設定情報ファイルを Kaspersky Endpoint Security ポリシーへインポートするウィンドウが表示されます。

設定情報ファイルを削除

このボタンをクリックすると、MDR 設定情報ファイルが Kaspersky Endpoint Security ポリシーから削除されます。

強制適用

【強制適用】スイッチをオンにすると、Kaspersky Endpoint Security は、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値の変更を禁止します。

【強制適用】スイッチをオフにすると、Kaspersky Endpoint Securityでは、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値が変更できます。

「Endpoint Detection and Response」 ウィンドウ

[すべて表示](#) | [すべて隠す](#)

Endpoint Detection and Response [?](#)

「Endpoint Managed Detection and Response」のスイッチで、Kaspersky Endpoint Managed Detection and Response サービスと対話する Endpoint Managed Detection and Response コンポーネントを有効または無効に設定できます。このソリューションは、新しい脆弱性攻撃、ランサムウェア、ファイルレス攻撃などの複雑な脅威からコンピューターを保護します。

「Endpoint Detection and Response」スイッチをオンにすると、Endpoint Detection and Response コンポーネントが有効になります。

「Endpoint Detection and Response」スイッチをオフにすると、Endpoint Detection and Response コンポーネントは無効になります。このスイッチは既定ではオフになっています。

「ネットワーク分離」セクションでは、セキュリティ侵害インジケーターの検知に応じてコンピュータをネットワークから分離するための設定を指定できます。

コンピュータのロック解除を設定する [?](#)

このリンクをクリックすると、[ネットワーク分離を自動的にオフにするまでの遅延を指定できるウィンドウ](#)が開きます。

除外リスト [?](#)

このリンクをクリックすると、[ネットワーク分離が自動的に有効になった後にコンピュータ上でブロックされないネットワーク接続を指定できるウィンドウ](#)が開きます。

「実行防止」セクションでは、実行可能ファイルとスクリプトの実行、および Office 形式のファイルのオープンに関する設定を構成できます。

実行防止 [?](#)

「実行防止」スイッチは、実行防止を有効または無効にします。

「実行防止」スイッチをオンにすると、実行防止ルールの一覧を作成および編集し、禁止されたオブジェクトが実行または開かれた時に実行される処理を選択できます。

「実行防止」スイッチをオフにすると、ユーザがデバイス上で実行したり開いたりするオブジェクトを管理することはできません。

このスイッチは既定ではオフになっています。

禁止されたオブジェクトを実行、または開いたときの処理 [?](#)

[ブロックしてレポートに書き込む \[?\]\(#\)](#)

このモードでは、防止ルールの基準に一致するオブジェクトの実行や、ドキュメントを開く動作がブロックされます。オブジェクトの実行の試行やドキュメントを開こうとする動作に関するイベントも、Kaspersky Security Center のイベントログと一元化されたログ記録システムに公開されます。

[イベントの記録のみ \[?\]\(#\)](#)

このモードを選択すると、Kaspersky Endpoint Security は防止ルールの条件に一致する実行可能オブジェクトの実行やドキュメントを開こうとする動作に関するイベントを Kaspersky Security Center イベントログと一元化されたログ記録システムに公開しますが、オブジェクトまたはドキュメントの実行や開く動作はブロックしません。既定では、このモードがオンです。

追加 [?](#)

このボタンをクリックすると、[新しい実行防止ルールを作成できるダイアログ](#)が開きます。

編集

このボタンをクリックすると、[既存の実行防止ルールを編集できるダイアログ](#)が開きます。

このボタンは、サーバのリストでサーバが選択されている場合に使用可能になります。

削除

このボタンをクリックすると、選択したルールがルールリストから削除されます。

このボタンは、サーバのリストでサーバが選択されている場合に使用可能になります。

「**Cloud Sandbox の設定**」セクションでは、Cloud Sandbox コンポーネントを有効または無効にすることができます。

Cloud Sandbox

「**Cloud Sandbox**」スイッチは、コンピュータ上の高度な脅威を検知するのに役立つ Cloud Sandbox 技術を有効または無効にします。Kaspersky Endpoint Security は、検知されたファイルを分析のために Cloud Sandbox に自動的に転送します。Cloud Sandbox はこれらのファイルを隔離された環境で実行し、悪意のある活動を識別してその評価を決定します。これらのファイルのデータは、Kaspersky Security Network に送信されます。したがって、Cloud Sandbox が悪意のあるファイルを検知した場合、Kaspersky Endpoint Security はこのファイルが検知されたすべてのコンピュータでこの脅威を排除するための適切な動作を実行します。

「**Cloud Sandbox**」スイッチをオンにすると、Cloud Sandbox 技術が有効になります。

「**Cloud Sandbox**」スイッチをオフにすると、Cloud Sandbox 技術は無効になります。

このスイッチは既定ではオフになっています。

強制適用

「**強制適用**」スイッチをオンにすると、Kaspersky Endpoint Security は、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値の変更を禁止します。

「**強制適用**」スイッチをオフにすると、Kaspersky Endpoint Security では、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値が変更できます。

「コンピュータのロック解除の設定」 ウィンドウ

[すべて表示](#) | [すべて隠す](#)

分離されたコンピュータのロックを自動的に解除するまでの時間

このチェックボックスは、指定された時間後にネットワーク分離を自動的にオフにする機能を有効または無効にします。

このチェックボックスをオンにすると、コンピュータのネットワーク分離を自動的にオフにするまでの遅延を指定できます。

このチェックボックスをオフにすると、Kaspersky Endpoint Security は隔離開始から 8 時間後にネットワーク隔離をオフにします。

既定では、このチェックボックスはオンです。

時間

ネットワーク分離が自動的にオフになるまでの間隔。

このフィールドは、「**分離されたコンピュータのロックを自動的に解除するまでの時間**」をオンにした場合にのみ編集できます。

「ネットワーク分離の除外」 ウィンドウ

[すべて表示](#) | [すべて隠す](#)

ネットワーク分離の除外リスト

このリストには、ネットワーク分離の除外として追加したネットワーク接続が含まれます。

追加

このボタンをクリックすると、[除外として追加するネットワーク接続の設定を手動で指定できるウインドウ](#)が開きます。

プロファイルから追加

このボタンをクリックすると、除外を設定するための標準ネットワークプロファイルを選択できるウインドウが開きます。

削除

このボタンをクリックすると、ネットワーク分離の除外リストからネットワーク接続が削除されます。

このボタンは、ネットワーク分離の除外リストで接続が選択されている場合に使用可能になります。

[ルールのオプション] ウインドウ

[すべて表示](#) | [すべて隠す](#)

ルール名

ネットワーク分離除外ルールの名前。

これはオプションの設定です。

方向

トラフィックの通信方向。

プロトコル

プロトコル種別

番号

プロトコル番号。

値は、[IANA（Internet Assigned Numbers Authority）が割り当てたインターネットプロトコル番号のリスト](#)  に準拠している必要があります。

このフィールドは、**カスタム**プロトコル種別を選択した場合に使用できます。

ローカルポートまたは範囲

ネットワーク分離の除外が設定されているコンピュータのローカルポートまたは範囲。

リモートポートまたは範囲

ネットワーク分離の除外が設定されているコンピュータのリモートポートまたは範囲。

リモートアドレス

ネットワーク分離の除外が設定されているコンピュータのネットワークアドレス。

アプリケーション

このチェックボックスを使用すると、分離されたコンピュータのネットワーク分離の除外に追加されたネットワーク接続を開始できるアプリケーションを追加できます。

このチェックボックスをオンにすると、そのようなアプリケーションを追加できます。

このチェックボックスをオフにすると、ネットワーク分離の除外に追加されたネットワーク接続は、分離されたコンピュータ上の任意のアプリケーションによって開始できるようになります。

既定では、このチェックボックスはオフです。

追加

このボタンをクリックすると、ネットワーク分離の除外に追加されたネットワーク接続を開始できるアプリケーションへのパスを指定できるウィンドウが開きます。

編集

このボタンをクリックすると、追加されたアプリケーションへのパスを編集できるウィンドウが開きます。

このボタンは、リストでアプリケーションが選択されている場合に使用可能になります。

削除

このボタンをクリックすると、追加されたアプリケーションが削除されます。

このボタンは、リストでアプリケーションが選択されている場合に使用可能になります。

[実行防止のルール] ウィンドウ

名前

ルール名。

種別

ブロックするオブジェクト種別。

「**オブジェクトのパス**」セクションでは、禁止するオブジェクトへの完全パスを指定するかどうかを選択できます。パスの指定を選択する場合は、対応するフィールドにその値を入力します。

「**オブジェクトのチェックサム**」セクションでは、禁止するオブジェクトのチェックサムを指定するかどうかを選択できます。チェックサムを指定する場合は、その種別を選択し、対応するフィールドに値を入力します。

[Endpoint Detection and Response (KATA)] ウィンドウ

[すべて表示](#) | [すべて隠す](#)

Endpoint Detection and Response (KATA)

「**Endpoint Detection and Response (KATA)**」スイッチは、Kaspersky Anti Targeted Attack Platform ソリューションと対話する Endpoint Detection and Response (KATA) コンポーネントを有効または無効にします。このソリューションは、標的型攻撃、高度な持続的脅威、ゼロデイ攻撃などの高度な脅威を迅速に検知します。

「**Endpoint Detection and Response (KATA)**」スイッチをオンにすると、Endpoint Detection and Response (KATA) コンポーネントが有効になります。

「**Endpoint Detection and Response (KATA)**」スイッチをオフにすると、Endpoint Detection and Response (KATA) コンポーネントは無効になります。

このスイッチは既定ではオフになっています。

サーバーの接続設定

このリンクをクリックすると [ダイアログが開き、KATA サーバーに接続するための設定を指定できます](#)。

KATA サーバー

このリストには、追加した KATA サーバーが含まれています。

追加

このボタンをクリックすると [ダイアログが開き、KATA サーバーへの接続を設定できます。](#)

編集

このボタンをクリックすると [ダイアログが開き、KATA サーバーへの既存の接続を編集できます。](#)
このボタンは、サーバのリストでサーバが選択されている場合に使用可能になります。

削除

このボタンをクリックすると、KATA サーバーがサーバのリストから削除されます。
このボタンは、サーバのリストでサーバが選択されている場合に使用可能になります。

アドレス

KATA サーバーの IP アドレス。

ポート

KATA サーバーのポート番号。

KATA サーバーに同期リクエストを送信する間隔（分）

KATA サーバーに送信される同期リクエストの間隔。
既定値は 5 分です。

イベントの送信時に TTL を使用する

Kaspersky Endpoint Security から KATA サーバーに送信されるパケットの TTL を有効または無効にします。TTL メカニズムは、イベントパケットの存続期間を [TTL（時間）] フィールドで指定された値に制限します。
このチェックボックスをオンにすると、TTL が有効になります。
このチェックボックスをオフにすると、TTL が無効になります。
既定では、このチェックボックスはオンです。

TTL（時間）

Kaspersky Endpoint Security によって KATA サーバーに送信されるパケットの存続期間。
既定値は 24 時間です。

[データ転送設定] セクションでは、KATA サーバーにデータを送信するための設定ができます。

最大イベント転送遅延時間（秒）

Kaspersky Endpoint Security が KATA サーバーにイベントを送信する間隔。
既定値は 30 秒です。

パケットごとのイベントの最大数

Kaspersky Endpoint Security によって KATA サーバーに送信されるパケットごとのイベントの最大数。
既定値は 1024 イベントです。

「**リクエストの調整**」セクションでは、送信されるイベントの数を制限できます。

リクエストの調整を有効にする

Kaspersky Endpoint Security によって KATA サーバーに送信されるイベントの数の制限を有効または無効にします。
このチェック ボックスをオンにすると、本製品によって送信されるイベントの数が制限されます。
このチェック ボックスをオフにすると、本製品によって送信されるイベントの数は制限されません。
既定では、このチェックボックスはオンです。

1時間ごとのイベントの最大数

Kaspersky Endpoint Security が KATA サーバーに1時間ごとに送信するイベントの最大数。Kaspersky Endpoint Security は1時間後にイベントの送信を再開します。
既定値は1時間あたり 3000 件です。

イベントの制限超過のパーセンテージ

同じ種別のイベントのしきい値（パーセンテージ）。
Kaspersky Endpoint Security は、イベントの総数に対する特定の種別のイベントの比率が設定されたしきい値を超えた場合、その種別のイベントの送信を制限します。
既定値は 15 パーセントです。

強制適用

「**強制適用**」スイッチをオンにすると、Kaspersky Endpoint Security は、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値の変更を禁止します。
「**強制適用**」スイッチをオフにすると、Kaspersky Endpoint Security では、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値が変更できます。

「KATA サーバー」 ウィンドウ

[すべて表示](#) | [すべて隠す](#)

アドレス

KATA サーバーの IP アドレス。

ポート

KATA サーバーのポート番号。
既定では 443 です。

「サーバーの接続設定」 ウィンドウ

[すべて表示](#) | [すべて隠す](#)

タイムアウト（秒）

KATA サーバーの応答タイムアウト。タイムアウトが経過すると、Kaspersky Endpoint Security は別の KATA サーバーへの接続を試行します。
既定値は 10 秒です。

「**サーバー TLS 証明書**」セクションでは、TLS 証明書の追加または削除、および追加した証明書に関する情報の表示が可能です。

TLS 証明書を追加

このボタンをクリックすると、KATA サーバーとの信頼済み接続の確立に使用する TLS 証明書を選択するウィンドウが表示されます。

削除

このボタンをクリックすると、現在の TLS 証明書が削除されます。

このボタンは、TLS 証明書が追加されている場合に使用できます。

「追加の接続セキュリティ」セクションでは、Kaspersky Endpoint Security と KATA サーバー間の接続の強化された保護を設定できます。

相互認証を使用する

Kaspersky Endpoint Security と KATA サーバー間の接続をより安全に保護する相互認証を有効または無効にします。相互認証を使用するには、暗号化されたコンテナを読み込む必要があります。

このチェックボックスをオンにすると、Kaspersky Endpoint Security は相互認証を使用して KATA サーバーに接続します。

このチェックボックスをオフにすると、Kaspersky Endpoint Security は KATA サーバーとの接続に相互認証を使用しません。

既定では、このチェックボックスはオフです。

暗号化されたコンテナを読み込む

このボタンをクリックすると、相互認証に使用する暗号化されたコンテナを選択するウィンドウが表示されます。暗号化されたコンテナの拡張子は .PFX です。

注意：暗号化されたコンテナはパスワードで保護されている必要があります。空のパスワードを使用して暗号化コンテナを追加することはできません。

暗号化されたコンテナのパスワード

相互認証に使用する暗号化されたコンテナのパスワード。

「セキュリティコントロール」セクション

[すべて表示](#) | [すべて隠す](#)

ウェブコントロール

「ウェブコントロール」スイッチでウェブコントロールを有効または無効にします。

「ウェブコントロール」スイッチをオンにすると、リモートコンピュータ上でユーザがアクセスする Web サイトを管理するルールが作成できます。

「ウェブコントロール」スイッチをオフにすると、リモートコンピュータ上でユーザがアクセスする Web サイトを管理するルールが作成できなくなります。

このスイッチは既定ではオフになっています。

ルールのリスト

リモートコンピュータ上でユーザがアクセスする Web サイトを管理するために作成したルールが含まれています。

ルールの並び順に従って、Kaspersky Endpoint Security が判断する適用の優先順位が決定されます。

追加

このボタンをクリックすると [ウィンドウが開き、ウェブコントロールの新しいルールを作成できます](#)。

削除

このボタンをクリックすると、選択したルールがルールのリストから削除されます。

このボタンは、ルールの隣のチェックボックスが選択されている場合に使用できます。

上へ

このボタンをクリックすると選択したルールが上に移動し、適用の優先度も上がります。

下へ

このボタンをクリックすると選択したルールが下に移動し、適用の優先度も下がります。

名前

ルール名。

ステータス

この列のスイッチで、ルールをアクティブにするかどうかを指定できます。
対応するルールに隣接するスイッチをオンまたはオフにして、ルールの状態を変更できます。

処理

ルールの対象である URL、URL グループ、または Web サイトのカテゴリに該当する URL へユーザがアクセスした時に本製品が実行する処理が表示されます。
この列の対応するショートカットメニューで別のオプションを選択すると、割り当てられたアクションを変更できます。

強制適用

〔強制適用〕スイッチをオンにすると、Kaspersky Endpoint Security は、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値の変更を禁止します。
〔強制適用〕スイッチをオフにすると、Kaspersky Endpoint Security では、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値が変更できます。

〔ルールを編集〕 ウィンドウ

[すべて表示](#) | [すべて隠す](#)

入力フィールドにルール名を入力

ルール名。

〔ステータス〕セクションでは、ルールをアクティブにするかどうかを設定できます。

アクティブ

このオプションをオンにすると、作成するルールが有効になります。リモートコンピュータにポリシーが強制適用されるとすぐに、ルールが適用されます。

非アクティブ

このオプションをオンにすると、作成するルールが無効になります。ポリシーが強制適用されると、ルールが一時停止状態になります。

〔処理〕セクションで、ルールの対象である URL、URL グループ、または Web サイトのカテゴリに該当する URL へのアクセス時に本製品が実行する処理を選択できます。

許可

このオプションをオンにすると、ルールの対象である URL、URL グループ、または Web サイトのカテゴリに該当する URL へのアクセスが許可されます。

注意：新規ポリシーウィザードウィンドウの〔ネットワーク〕セクションで〔セキュアな接続（HTTPS）をチェック〕スイッチをオンにすると、リモートコンピュータからの Web サイトへのアクセスが許可されます。

既定では、このオプションがオンです。

ブロック

このオプションをオンにすると、ルールの対象である URL、URL グループ、または Web サイトのカテゴリに該当する URL へのアクセスが防止されます。

注意：新規ポリシーウィザードのウィンドウの [ネットワーク] セクションで [セキュアな接続 (HTTPS) をチェック] スイッチをオンにすると、リモートコンピュータ上でウェブコントロールがブロックする Web サイトにユーザがアクセスすると通知が表示されます。

警告を表示 [?](#)

このオプションをオンにすると、ルールの対象である URL、URL グループ、または Web サイトのカテゴリに該当する URL へユーザがアクセスしようすると警告を表示します。

[ルール範囲] セクションで、ルールの対象を特定の URL にするか、URL のグループにするか、Web サイトのカテゴリにするかを選択できます。

カテゴリ [?](#)

このオプションをオンにすると、作成するルールの対象が Web サイトのカテゴリになります。

カテゴリを選択 [?](#)

このリンクをクリックすると、[ダイアログが開き、ルールの影響を受ける Web サイトのカテゴリを選択できます。](#)

個別のアドレス [?](#)

このオプションをオンにすると、作成するルールの対象が特定の URL または URL のグループになります。

既定では、このオプションがオンです。

追加 [?](#)

このボタンをクリックすると、[ダイアログが開き、ルールの対象である URL または URL マスクを指定できます。](#)

削除 [?](#)

このボタンをクリックすると、選択したルールの対象である URL または URL マスクが、URL のリストから削除されます。
このボタンは、URL または URL マスクの隣のチェックボックスが選択されている場合に使用できます。

アドレス [?](#)

ルールの対象である URL または URL マスク。

[URL を追加] ダイアログ

[すべて表示](#) | [すべて隠す](#)

URL の入力フィールドに入力する [?](#)

ルールの影響を受ける URL または URL マスク。

[コンテンツカテゴリ] ダイアログ

[すべて表示](#) | [すべて隠す](#)

コンテンツカテゴリのリスト [?](#)

ルールに追加可能な Web サイトのカテゴリリストが含まれています。

Web サイトのカテゴリ名に隣接するチェックボックスを選択して、そのカテゴリに該当する Web サイトをルールに追加したり、ルールから削除したりできます。

これらのチェックボックスは既定ではオフになっています。

「脅威対策」セクション

[すべて表示](#) | [すべて隠す](#)

ファイル脅威対策

このリンクをクリックすると [ウィンドウが開き、ファイル脅威対策の設定を設定できます。](#)

ウェブ脅威対策

このボタンをクリックすると [ウィンドウが開き、ウェブ脅威対策の設定を設定できます。](#)

ネットワーク脅威対策

このボタンをクリックすると [ウィンドウが開き、ネットワーク脅威対策の設定を設定できます。](#)

メール脅威対策

このリンクをクリックするとウィンドウが開き、メール脅威対策の設定を設定できます。

ファイアウォール

このリンクをクリックするとウィンドウが開き、ファイアウォールの設定を設定できます。

「ファイル脅威対策」ウィンドウ

[すべて表示](#) | [すべて隠す](#)

ファイル脅威対策

「**ファイル脅威対策**」スイッチにより、ファイル脅威対策を有効または無効にします。

「**ファイル脅威対策**」スイッチをオンにすると、Kaspersky Endpoint Security はポリシーが適用されるクライアントコンピュータに対してファイルシステムのリアルタイム監視を実行します。

「**ファイル脅威対策**」スイッチがオフになっていると、Kaspersky Endpoint Security はポリシーが適用されるクライアントコンピュータのファイルシステムを保護しません。

このスイッチは既定ではオンになっています。

「**保護範囲**」セクションでは、事前に設定された項目の1つを選択するか、選択したファイルまたはフォルダを追加することにより、保護範囲を設定できます。

追加

クリックすると [ダイアログが開き、保護範囲に含めるオブジェクトのリストに、ファイル、フォルダ、またはマスクを指定できます。](#)

削除

保護範囲からオブジェクトを削除します。

このボタンは、保護対象のオブジェクトのリストでオブジェクトが選択されている場合に使用可能になります。

既定で保護範囲に含まれているオブジェクトは削除できません。

保護範囲

この列には、ファイル脅威対策が有効になっている時に Kaspersky Endpoint Security がスキャンするオブジェクトが表示されます。

既定では、Kaspersky Endpoint Security は次のオブジェクトをスキャンします：

- **すべてのリムーバブルディスク。** Kaspersky Endpoint Security はすべてのリムーバブルドライブをスキャンします。
- **すべての内部ディスク。** Kaspersky Endpoint Security は、すべての内部ディスクをスキャンします。
- **すべてのネットワークディスク。** Kaspersky Endpoint Security は、すべてのネットワークドライブをスキャンします。

ステータス

この列のスイッチがオンになっており、ファイル脅威対策が有効になっている場合、Kaspersky Endpoint Security は **〔保護範囲〕** 列の対応するオブジェクトをスキャンします。

この列のスイッチがオフになっており、ファイル脅威対策が有効になっている場合、Kaspersky Endpoint Security は **〔保護範囲〕** 列の対応するオブジェクトをスキャンしません。

詳細

この列は、Kaspersky Endpoint Security が対応するオブジェクトのサブフォルダをスキャンするかどうかを示します。

〔悪意のあるオブジェクトが検知された場合〕 セクションでは、Kaspersky Endpoint Security が悪意のあるオブジェクトを検知した時に実行する動作を選択できます。

手動選択

ファイルに感染した悪意のあるオブジェクトの情報が通知ウィンドウに表示され、実行する処理を選択するよう要求されます。処理は、オブジェクトのステータスによって異なる場合があります。

既定では、このオプションがオンです。

駆除、駆除できない場合は削除

感染したファイルへのアクセスをブロックし、ユーザの確認を要求せずにファイルを自動的に駆除します。

駆除したファイルは、元の保存場所に元のファイル名で保存されます。駆除に失敗すると、Kaspersky Endpoint Security は感染したファイルを削除します。

駆除、駆除できない場合はブロック

感染したファイルへのアクセスをブロックし、ユーザの確認を要求せずにファイルを自動的に駆除します。

駆除したファイルは、元の保存場所に元のファイル名で保存されます。駆除に失敗した場合、感染したファイルはブロックした状態で元の保存場所に置かれます。

〔最適化〕 セクションでは、スキャンのパフォーマンスを設定し、スキャン技術を選択できます。

新しいファイルと変更されたファイルのみスキャンする

このチェックボックスは、新しいファイルまたは前回のスキャン以降に変更されたファイルとして認識したファイルのみのスキャンを有効または無効にします。

このチェックボックスをオンにすると、新しいファイルまたは前回のスキャン以降に変更されたファイルとして認識されたファイルのみをスキャンします。

このチェックボックスをオフにすると、すべてのファイルをスキャンします。

既定では、このチェックボックスはオンです。

読み取り専用システムボリュームのスキャンをスキップする

読み取り専用のシステムボリュームのスキャンをスキャンするかどうかを選択します。

このチェックボックスをオンにすると、読み取り専用のシステムボリュームのスキャンがスキップされ、スキャンにかかる時間が大幅に短縮されます。

このチェックボックスをオフにすると、読み取り専用のシステムボリュームをスキャンします。

既定では、このチェックボックスはオンです。

iSwift を使用

スキャン中に iSwift 技術を使用するかどうかを選択します。iSwift では、特別なアルゴリズムを使用して特定のオブジェクトをスキャンから除外します。これにより、スキャン速度を上げることができます。

このチェックボックスをオンにすると、スキャン中に iSwift 技術を使用します。

このチェックボックスをオフにすると、スキャン中に iSwift 技術を使用しません。

既定では、このチェックボックスはオンです。

【ファイル種別】 セクションでは、ファイル脅威対策が有効になっている場合、Kaspersky Endpoint Security でスキャンするファイルを選択できます。

すべてのファイルをスキャン [?](#)

実行中のファイルシステムオブジェクト、開いているファイルシステムオブジェクト、保存されたファイルシステムオブジェクトをすべてスキャンします。

アプリケーションとドキュメントをスキャン（内容で判断） [?](#)

感染の可能性があるオブジェクトのみをその内容に基づいてスキャンします。

アプリケーションとドキュメントをスキャン（拡張子で判断） [?](#)

感染の可能性があるオブジェクトのみをファイルの拡張子に基づいてスキャンします。
拡張子のリストはカスペルスキーが定義し、Kaspersky Endpoint Security の定義データベースに含まれます。
拡張子なしのファイルは常時スキャンされます。

【複合ファイル】 セクションでは、ファイル脅威対策が有効になっている場合、Kaspersky Endpoint Security でスキャンする複合ファイルの種別を選択できます。

圧縮ファイルをスキャンする [?](#)

圧縮ファイルのスキャンを有効または無効にします。拡張子のリストについては、Kaspersky Endpoint Security のヘルプを参照してください。
このチェックボックスをオンにすると、圧縮ファイルをスキャンします。
このチェックボックスをオフにすると、スキャン中に圧縮ファイルをスキップします。

インストールパッケージをスキャンする [?](#)

インストールパッケージのスキャンを有効または無効にします。
このチェックボックスをオンにすると、インストールパッケージをスキャンします。
このチェックボックスをオフにすると、スキャン中にインストールパッケージをスキップします。

OLE 埋め込みオブジェクトをスキャンする [?](#)

Excel スプレッドシート、マクロ、メールの添付ファイルなど、ファイルに埋め込まれたオブジェクトをスキャンするかどうかを選択します。
このチェックボックスをオンにすると、埋め込み OLE オブジェクトをスキャンします。
このチェックボックスをオフにすると、スキャン中に埋め込み OLE オブジェクトをスキップします。

次のサイズより大きい圧縮ファイルを展開しない [?](#)

スキャンする圧縮ファイルのサイズを制限するかどうかを選択できます。
このチェックボックスをオンにすると、スキャン中、指定された値よりも大きい圧縮ファイルをスキップします。
このチェックボックスをオフにすると、サイズに関係なく常に圧縮ファイルを解凍してスキャンします。
このチェックボックスは、【圧縮ファイルをスキャンする】をオンにすると使用可能になります。

次のサイズより大きい圧縮ファイルの展開を延期する [?](#)

このオプションでは、スキャンする圧縮ファイルのサイズを制限します。
このチェックボックスをオンにすると、設定されたサイズ制限を超える圧縮ファイルをすべてスキャンしますが、そのような圧縮ファイルが検出された 2 分後に低い優先度で実行します。
このチェックボックスをオフにすると、すべての圧縮ファイルを同じ優先度でスキャンします。
このチェックボックスは、【圧縮ファイルをスキャンする】をオンにすると使用可能になります。

強制適用 [?](#)

【強制適用】スイッチをオンにすると、Kaspersky Endpoint Security は、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値の変更を禁止します。

【強制適用】スイッチをオフにすると、Kaspersky Endpoint Security では、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値が変更できます。

「保護範囲を追加」 ダイアログ

[すべて表示](#) | [すべて隠す](#)

ファイル名、フォルダ名、またはマスクを入力

ファイルやフォルダのパス、またはファイルやフォルダのマスク。

フォルダ名

オブジェクトをフォルダとしてスキャンするかどうかを選択します。

このチェックボックスをオンにすると、「ファイル名、フォルダ名、またはマスクを入力」で指定したオブジェクトをフォルダとしてスキャンします。

このチェックボックスをオフにすると、「ファイル名、フォルダ名、またはマスクを入力」で指定したオブジェクトをファイルとしてスキャンします。

既定では、このチェックボックスはオンです。

サブフォルダを含める

このチェックボックスは、「ファイル名、フォルダ名、またはマスクを入力」で指定したフォルダのサブフォルダのスキャンを有効または無効にします。

このチェックボックスをオンにすると、マルウェアスキャン中にサブフォルダをスキャンします。

このチェックボックスをオフにすると、「ファイル名、フォルダ名、またはマスクを入力」フィールドで指定したフォルダのみをマルウェアスキャン中にスキャンします。

既定では、このチェックボックスはオンです。

「ウェブ脅威対策」 ウィンドウ

[すべて表示](#) | [すべて隠す](#)

ウェブ脅威対策

【ウェブ脅威対策】スイッチにより、ウェブ脅威対策を有効または無効にします。

【ウェブ脅威対策】スイッチをオンにすると、Safari、Google Chrome、または Firefox ブラウザで HTTP および HTTPS プロトコルを使用して、コンピュータが送受信するデータを、ウェブ脅威対策でスキャンします。

【ウェブ脅威対策】スイッチをオフにすると、コンピュータが Web ブラウザで送受信するデータを、ウェブ脅威対策でスキャンしません。
このスイッチは既定ではオンになっています。

【悪意のあるオブジェクトが検知された場合】セクションでは、Kaspersky Endpoint Security が悪意のあるオブジェクトを検知した時に実行する動作を選択できます。

手動選択

Web トラフィックオブジェクトに感染したマルウェアの種別の情報が通知ウィンドウに表示され、このオブジェクトに実行する処理を選択するよう要求されます。実行可能な処理は、オブジェクトの状態によって異なる場合があります。

既定では、この処理が選択されています。

自動的にブロック

危険な Web トラフィックオブジェクトへのアクセスを自動的にブロックします。

【信頼する URL】セクションで、信頼できる URL のリストを作成または編集し、このリストの Web アドレスからのトラフィックのスキャンを有効または無効にすることができます。

信頼する URL からの Web トラフィックをスキャンしない

信頼する URL からの Web トラフィックをスキャンするかどうかを選択します。

このチェックボックスをオンにすると、信頼する URL からの Web トラフィックはスキャンされません。

このチェックボックスをオフにすると、信頼する URL からの Web トラフィックをスキャンします。

既定では、このチェックボックスはオフです。

URL のリスト [?](#)

信頼する URL のリストが表示されます。

リストの URL に隣接するチェックボックスをオフにできます。このチェックボックスをオフにすると、ウェブ脅威対策は URL からの Web トラフィックをスキャンします。

「信頼する URL からの Web トラフィックをスキャンしない」をオンにすると、このリストが使用可能になります。

追加 [?](#)

クリックすると [ダイアログが開き、信頼する URL のリストに追加する URL、または URL のマスクを入力できます。](#)

削除 [?](#)

このボタンをクリックすると、選択した URL、または URL のマスクが、信頼する URL のリストから削除されます。

信頼する URL のリストで、URL、または URL のマスクが選択されていると、このボタンが使用可能になります。

URL [?](#)

この列には、信頼する URL が表示されます。

ステータス [?](#)

この列のスイッチをオンにすると、ウェブ脅威対策が有効で、「信頼する URL からの Web トラフィックをスキャンしない」をオンにすると、Kaspersky Endpoint Security は「URL」列からの対応するオブジェクトをスキャンしません。

この列のスイッチをオフにすると、ウェブ脅威対策が有効で、「信頼する URL からの Web トラフィックをスキャンしない」をオンにすると、Kaspersky Endpoint Security は「URL」列からの対応するオブジェクトをスキャンします。

強制適用 [?](#)

「強制適用」スイッチをオンにすると、Kaspersky Endpoint Security は、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値の変更を禁止します。

「強制適用」スイッチをオフにすると、Kaspersky Endpoint Security では、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値が変更できます。

「URL を追加」ダイアログ

[すべて表示](#) | [すべて隠す](#)

URL の入力フィールドに入力する [?](#)

ウェブ脅威対策でトラフィックをスキャンしない URL または URL マスク。

「ステータス」セクションで、Kaspersky Endpoint Security がこの URL や URL グループからのトラフィックをスキャンするかどうかを指定できます。

無効 [?](#)

URL または URL マスクが「信頼する URL」のリストに追加されますが、Kaspersky Endpoint Security はそのトラフィックをスキャンしません。

有効 [?](#)

URL または URL マスクが「信頼する URL」のリストに追加され、Kaspersky Endpoint Security はそのトラフィックをスキャンしません。

[ネットワーク脅威対策] ウインドウ

[すべて表示](#) | [すべて隠す](#)

ネットワーク脅威対策

[ネットワーク脅威対策] スイッチにより、ネットワーク脅威対策を有効または無効にします。

[ネットワーク脅威対策] スイッチをオンにすると、Kaspersky Endpoint Security は、リモートコンピュータをネットワーク上からの攻撃から保護します。

[ネットワーク脅威対策] スイッチをオフにすると、Kaspersky Endpoint Security は、リモートコンピュータをネットワーク上からの攻撃から保護しません。

このスイッチは既定ではオンになっています。

[ネットワーク脅威対策の設定] セクションでは、Kaspersky Endpoint Security がコンピュータからの攻撃をブロックする時間を変更できます。

攻撃を行っているコンピュータをブロックする時間

攻撃元のコンピュータをブロック対象のコンピュータのリストに期間を指定して追加するかどうかを選択します。

このチェックボックスをオンにすると、指定された期間中、ブロックするコンピュータのリストに攻撃元のコンピュータを追加します。

このチェックボックスをオフにすると、攻撃元のコンピュータをブロックしません。

既定では、このチェックボックスはオンです。

既定では、攻撃元のコンピュータは 60 秒間ブロックされます。

[除外リスト] セクションでは、ネットワーク活動が Kaspersky Endpoint Security によってブロックされないリモートコンピュータの IP アドレスのリストを作成または編集できます。

IP アドレスのリスト

ネットワークの動作を本製品でブロックしないリモートコンピュータの IP アドレスが表示されます。

追加

このボタンをクリックすると [ダイアログが開き、リモートコンピュータの IP アドレスを入力できます](#)。

削除

このボタンをクリックすると、選択した IP アドレスが、IP アドレスのリストから削除されます。

IP アドレスのリストでリモートコンピュータの IP アドレスが選択されていると、このボタンが使用可能になります。

強制適用

[強制適用] スイッチをオンにすると、Kaspersky Endpoint Security は、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値の変更を禁止します。

[強制適用] スイッチをオフにすると、Kaspersky Endpoint Security では、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値が変更できます。

[除外を追加] ダイアログ

[すべて表示](#) | [すべて隠す](#)

IP アドレスの入力フィールドに入力する

リモートコンピュータの IP アドレス。

[先進の脅威対策] セクション

[すべて表示](#) | [すべて隠す](#)

[KSN 設定] セクションでは、Kaspersky Security Network の使用を設定できます。

「Kaspersky Security Network」スイッチにより、Kaspersky Security Network に参加するかどうかを選択します。

「Kaspersky Security Network」スイッチをオンにすると、ポリシーが適用されたクライアントコンピュータは Kaspersky Security Network へ参加します。

「Kaspersky Security Network」スイッチをオフにすると、ポリシーが適用されたクライアントコンピュータは Kaspersky Security Network へ参加しません。

このスイッチは既定ではオフになっています。

拡張 KSN モード ②

「拡張 KSN モード」のスイッチで、クライアントコンピュータの保護機能と Kaspersky Endpoint Security のユーザビリティの向上に必要な追加のデータをリモートコンピュータからカスペルスキーに送信するかどうかを選択します。

「拡張 KSN モード」をオンにすると、ポリシーを適用したクライアントコンピュータから検知サービスの動作に必要なデータおよび追加のデータが Kaspersky Security Network に提供されます。

「拡張 KSN モード」をオフにすると、ポリシーを適用したクライアントコンピュータから検知サービスの動作に必要なデータのみが Kaspersky Security Network に提供され、追加のデータは提供されません。

「拡張 KSN モード」スイッチは既定ではオフになっています。

このスイッチは「Kaspersky Security Network」スイッチをオンにすると自動的にオンになりますが、オフにすることもできます。

グローバル KSN インフラストラクチャの Kaspersky Security Network の使用時にカスペルスキーに提供されるデータ ②

「Kaspersky Security Network」スイッチを有効にし、「拡張 KSN モード」スイッチを無効にすると、クライアントコンピュータで実行中の本製品がカスペルスキーに次のデータを提供します：

- 適用されているライセンスの情報：ライセンスの種別および有効期間、ライセンスの有効期限までの日数、ライセンスの購入元である代理店の識別子、地域のアクティベーションセンターの識別子、アクティベーションコードのチェックサム、SHA1 アルゴリズムを使用して計算されたチケットボディのハッシュ、ライセンスチケットの作成日時、ライセンス情報の識別子、ライセンスチケットの識別子、ライセンスチケットのシーケンスの識別子、ユーザのコンピュータの一意な識別子、ライセンスチケットが有効になった日付、ライセンスチケットの有効期限、ライセンスチケットの現在のステータス、チケットヘッダーのバージョン、ライセンスのバージョン、チケットヘッダーの署名に使用された証明書の識別子、ライセンスファイルのチェックサム、チケットヘッダーの署名元のシリアル番号、認証トークン。
- インストールされた本ソフトウェアの詳細バージョン。

インストールされた本ソフトウェアの種別。ソフトウェアアップデートの ID。評価サービスの ID。プロトコルタイプの ID。地域のアクティベーションセンターの ID。本ソフトウェアのサービスの決定のうち取り消されたもののリストのバージョン。トリガーされた本ソフトウェアの定義データベースのレコードの ID。トリガーされた本ソフトウェアの定義データベースのレコードのタイムスタンプ。トリガーされた本ソフトウェアの定義データベースのレコードの種別。本ソフトウェアのコンピュータへのインストールのインスタンスの一意な ID。ライセンスがアクティベートされた日付。ライセンスの有効期限日。ライセンスの識別子。本ソフトウェアが使用中のライセンスのステータス。処理中のオブジェクトのチェックサム種別。検知されたマルウェアの名前、ユーザのコンピュータまたはデータに損害を与える目的で使用される可能性がある正規のソフトウェアの名前。処理中のオブジェクトのチェックサム。本ソフトウェアのアクティベーションコードのチェックサム。本ソフトウェアの詳細バージョン。一意のデバイス ID。本ソフトウェアの ID。本ソフトウェアのライセンス情報ファイルのチェックサム。本ソフトウェアのライセンスの提供に使用された情報形式の ID。本ソフトウェアのライセンスチケットのヘッダーへの署名に使用される証明書の識別子。本ソフトウェアのライセンスチケットの作成日時。本ソフトウェアのライセンスチケットのチェックサム。本ソフトウェアのライセンスチケットのバージョン。本ソフトウェアのアクティベーションコードのバージョン。権利者のインフラストラクチャへのリクエストに含まれるデータの形式。使用中のライセンスチケットの ID。本ソフトウェアのコンポーネントの ID。本ソフトウェアの動作の結果。エラーコード。アクセスされた Web サービスのアドレス (URL、IP)。ポート番号。Web サービスのリクエスト元の URL (リファラー)。証明書の公開鍵。スキャンされたオブジェクトのデジタル証明書のサムプリントとハッシュアルゴリズム。

「Kaspersky Security Network」と「拡張 KSN モード」のスイッチを有効にすると、クライアントコンピュータで実行中の本製品がカスペルスキーに次のデータを提供します：

- コンピュータにインストールされているオペレーティングシステム (OS) やサービスパックのバージョンに関する情報、OS カーネルファイルのバージョンおよびチェックサム (MD5、SHA2-256、SHA1)、OS 実行モードの識別子。OS のバージョン、OS のビルド番号、OS のアップデート番号、OS のエディション、OS のエディションに関する詳細情報。OS のサービスパックのバージョン OS の起動日時。ふるまい分析のサブシステムにおける OS 動作に関するイベントの処理遅延時間。現在の種別の遅延された OS 動作イベントの数。プロアクティブディフェンスのサブシステムにおける OS 動作に関するイベントの処理遅延時間。処理された OS 動作イベントの数。処理された OS 同期動作イベントの数。現在の種別のすべての OS 動作イベントの合計遅延時間。持続的イベントを記憶するサブシステムにおける、OS 動作に関するイベントの処理遅延時間。すべての OS 動作イベントの合計遅延。待機中の OS 同期動作イベントの数。OS 内の動作イベントを受信した日時。
- 以前、OS の再起動が失敗した履歴：再起動に失敗した回数。
- インストールされている本製品に関する情報およびアンチウイルス保護状況：ソフトウェアのインストール識別子 (PCID) 本ソフトウェアの定義データベースのレコードのバージョン、コンピューター上にインストールされたアプリケーションのインスタンスの一意な識別子、アプリケーションの種別、アプリケーション種別の識別子、インストールされたアプリケーションの詳細バージョン、アプリケーションの設定のバージョンの識別子、コンピューター種別の識別子、アプリケーションがインストールされたコンピューターの一意な識別子、権利者のサービスにおける一意なユーザー識別子、言語および動作状況、インストールされたソフトウェアコンポーネントのバージョンと動作状況、権利者のサービスに接続するために使用されたプロトコルのバージョン、インストールされた本ソフトウェアの詳細バージョン。インストールされた本ソフトウェアの種別。ソフトウェアアップデートの ID。評価サービスの ID。プロトコルタイプの ID。地域のアクティベーションセンターの ID。本ソフトウェアのサービスの決定のうち

取り消されたもののリストのバージョン。トリガーされた本ソフトウェアの定義データベースのレコードの ID。トリガーされた本ソフトウェアの定義データベースのレコードのタイムスタンプ。トリガーされた本ソフトウェアの定義データベースのレコードの種別。本ソフトウェアのコンピュータへのインストールのインスタンスの一意な ID。ライセンスがアクティベートされた日付。ライセンスの有効期限日。ライセンスの識別子。本ソフトウェアが使用中のライセンスのステータス。処理中のオブジェクトのチェックサム種別。検知されたマルウェアの名前、ユーザのコンピュータまたはデータに損害を与える目的で使用される可能性がある正規のソフトウェアの名前。処理中のオブジェクトのチェックサム。本ソフトウェアのアクティベーションコードのチェックサム。本ソフトウェアの詳細バージョン。本ソフトウェアの ID。本ソフトウェアのライセンス情報ファイルのチェックサム。本ソフトウェアのライセンスの提供に使用された情報形式の ID。本ソフトウェアのライセンスチケットのヘッダーへの署名に使用される証明書の識別子。本ソフトウェアのライセンスチケットの作成日時。本ソフトウェアのライセンスチケットのチェックサム。本ソフトウェアのライセンスチケットのバージョン。本ソフトウェアのアクティベーションコードのバージョン。権利者のインフラストラクチャへのリクエストに含まれるデータの形式。使用中のライセンスチケットの ID。本ソフトウェアのコンポーネントの ID。本ソフトウェアの動作の結果。エラーコード。アクセスされた Web サービスのアドレス (URL、IP)。ポート番号。Web サービスのリクエスト元の URL (リファラー)。定義データベースのアップデートと適用のサイクル数。定義データベースが最後にアップデートおよび適用された日時。本ソフトウェアの定義データベースの公開日時。本ソフトウェアのコンポーネントのバージョン。ソフトウェアアップデートの ID。インストールされた本ソフトウェアの種別。システムウォッチャーの開始日時。本ソフトウェアのインストール日時。システムウォッチャーによって統計が送信される確率。システムウォッチャーによる標準処理時間よりも長い時間がかかったイベントのコード。システムウォッチャーによる標準処理時間を超えたイベントのデータベース処理時間。システムウォッチャーによるイベントの処理に許可される最大時間。システムウォッチャーによる標準処理時間を超えたイベントの処理時間。システムウォッチャーによる標準処理時間よりも長い時間がかかったイベントの総数。

- 処理したすべてのオブジェクトおよび操作に関する情報：処理中のオブジェクトに対する本ソフトウェアの判定、ディレクトリコード、処理中のオブジェクトのサイズ、処理中のオブジェクトのチェックサム (SHA256)、システムウォッチャーを使用して検知されたソフトウェアの数、システムウォッチャーでソフトウェアを検知した日時、検知の特性、トリガーされた本ソフトウェアの定義データベースのレコードの ID。システムウォッチャーでソフトウェアを検知した理由、処理中のオブジェクトのチェックサム (MD5)、モジュールの整合性チェックの結果、処理中のオブジェクトの名前、トリガーされた本ソフトウェアの定義データベースのレコードの種別、処理中のオブジェクトへのパス。スキャンしたオブジェクトの製造元の名前、スキャンの日時、URL およびダウンロードされたリファラーのアドレス、スキャンされたファイルのサイズおよびパス、アーカイブかどうかのフラグ、ファイルの作成日時、圧縮されていた場合はバッカーの名前、サイズおよびチェックサム (MD5、SHA2-256)、ファイルのエントロピー、ファイルの種別、ファイル種別コード、ファイルが実行可能であるかどうかのフラグ、識別子および形式、オブジェクトのチェックサム (MD5、SHA2-256)、オブジェクトの追加チェックサムの種別および値、オブジェクトのデジタル署名 (証明書) に関するデータ：証明書の発行元に関する情報、前回の統計が送信されてからオブジェクトが実行された回数、本製品のスキャンタスクの識別子、オブジェクトの評価に関する情報の受信手段、TARGET フィルターの値、適用可能な検知技術の技術的パラメータ。処理中のオブジェクトへのパス。ディレクトリコード。
- 実行ファイルの場合：ファイルセクションの情報量、評価の検証フラグまたはファイルの署名フラグ、検証対象のオブジェクトに読み込まれたアプリケーションの名前、種別、ID 種別、チェックサム (MD5) およびサイズ、アプリケーションのパスおよびテンプレートのパス、自動実行リストの署名、エントリの日時、属性のリスト、圧縮ソフトウェアの名前、アプリケーションのデジタル署名に関する情報：発行者の証明書、アップロードされたファイルの MIME 形式での名前、ファイルが作成された日時。
- 実行中のアプリケーションおよびそのモジュールに関する情報：実行中のファイルのチェックサム (MD5、SHA2-256)、ファイルのサイズ、属性、作成日時、圧縮ソフトウェアの名前 (ファイルが圧縮されている場合)、ファイル名、システム上で実行されているプロセスに関する情報 (プロセス ID (PID)、プロセス名、プロセスを開始したアカウントに関する情報、プロセスを開始したアプリケーションおよびコマンド、プロセスのファイルへの完全パスおよび開始したコマンドライン、プロセスが属するアプリケーションの説明 (アプリケーション名および配信元の情報)、使用されるデジタル証明書およびそれらの正当性を検証するために必要な情報またはファイルのデジタル署名が存在しない旨のフラグ)、プロセスに読み込まれたモジュールの情報：名前、サイズ、種別、作成日、属性、チェックサム (MD5、SHA2-256、SHA1) およびパス、PE ファイルのヘッダー情報、圧縮ソフトウェア名 (ファイルが圧縮されている場合)、統計情報の有効性および使用可否に関する情報、送信される統計情報の生成条件の識別子。
- 脅威または脆弱性が検知された場合、検知されたオブジェクトに関する情報に加え、次の情報が提供されます：定義データベース中のレコードの識別子、バージョンおよび種別、カスペルスキーの分類による脅威名、定義データベースの最終アップデート日時、実行ファイルの名前、脅威が検知された URL をリクエストしたアプリケーションのファイルのチェックサム (MD5)、検知した脅威の IP アドレス (IPv4 または IPv6)、脆弱性の識別子および脅威レベル、脅威を検知した Web ページの URL およびリファラー。
- 悪意のある可能性があるオブジェクトが検知された場合、プロセスのメモリ内のデータに関する情報が提供されます。
- ネットワーク攻撃の情報：攻撃元コンピュータの IP アドレスおよびユーザのコンピュータ上でネットワーク攻撃の標的にされたポート番号、攻撃プロトコルの ID、名前および攻撃種別。
- ネットワーク接続に関する情報：ポートを開いたプロセスを起動したファイルのバージョンおよびチェックサム (MD5、SHA2-256、SHA1)、プロセスのファイルのパスおよびデジタル署名、ローカルおよびリモートの IP アドレス、ローカルおよびリモート接続のポート番号、接続状況、ポートが開かれた時刻。
- 危険なオブジェクトまたは疑わしいオブジェクトを検知した Web ページの URL および IP アドレス、この URL をリクエストしたファイルの名前、サイズおよびチェックサム、識別子、検知結果の決定基準に使用されたルールの重み係数および度数、攻撃の目的に関する情報。
- インストール済み本ソフトウェアおよび定義データベースのアップデートに関する情報：アップデートタスクの完了状況、アップデート中に発生した可能性のあるエラーの種別、失敗したアップデートの数、アップデートを実行した本ソフトウェア機能の識別子。
- Kaspersky Security Network (KSN) の使用に関する情報：KSN の識別子、本ソフトウェアの識別子、本ソフトウェアの詳細バージョン、個人を特定できないようにしたお客様のデバイスの IP アドレス、KSN へのリクエストの実行品質を示す指数、KSN 用パケットの処理品質を示す指数、KSN へのリクエストの件数およびリクエストの種別に関する情報、統計情報の送信を開始した日時と終了した日時、KSN 設定のアップデートに関する情報：アクティブな設定の識別子、受信した設定の識別子、設定のアップデートのエラーコード。

- ・ イベントに関するシステムログ内の情報： イベントのタイムスタンプ、 イベントが検知されたログの名前、 イベントの種別およびカテゴリ、 イベントの発生源の名前およびイベントの説明。
- ・ ファイルおよび URL の評価決定に関する情報： 評価が要求された URL とその参照元、 接続のプロトコルタイプ、 アプリケーション種別の内部識別子、 使用されているポートの番号、 ユーザ識別子、 スキャンされたファイルのチェックサム (MD5)、 検知された脅威の種別、 脅威の検知に使用したレコードに関する情報 (定義データベースのレコードの識別子、 レコードのタイムスタンプと種別)。 証明書の公開鍵。 スキャンされたオブジェクトのデジタル証明書のサムプリントとハッシュアルゴリズム。
- ・ 本ソフトウェアの地域分布に関する情報： 本ソフトウェアのインストールおよびアクティベーションの日時、 本ソフトウェアのアクティベーション用のライセンスを提供した代理店の識別子、 本ソフトウェアの識別子、 本ソフトウェアの言語版の識別子、 本ソフトウェアに適用されたライセンスの識別番号、 KSN に参加しているかどうかのフラグ。
- ・ 適用されているライセンスの情報： ライセンスの種別および有効期間、 ライセンスの有効期限までの日数、 ライセンスの購入元である代理店の識別子、 地域のアクティベーションセンターの識別子、 アクティベーションコードのチェックサム、 SHA1 アルゴリズムを使用して計算されたチケットボディのハッシュ、 ライセンスチケットの作成日時、 ライセンス情報の識別子、 ライセンスチケットの識別子、 ライセンスチケットのシーケンスの識別子、 ユーザのコンピュータの一意な識別子、 ライセンスチケットが有効になった日付、 ライセンスチケットの有効期限、 ライセンスチケットの現在のステータス、 チケットヘッダーのバージョン、 ライセンスのバージョン、 チケットヘッダーの署名に使用された証明書の識別子、 ライセンスファイルのチェックサム、 チケットヘッダーの署名元のシリアル番号、 認証トークン。
- ・ コンピュータにインストールされているハードウェアに関する情報： 搭載または接続された装置の種別、 名前、 機種名、 ファームウェアのバージョン、 パラメータ。
- ・ 端末に関する情報： 端末の識別子。
- ・ ウェブコントロール機能の動作に関する情報：
機能のバージョン、 当該カテゴリに分類された理由および関連情報、 分類された URL、 ブロックまたは分類されたオブジェクトのホストの IP アドレス。

クラウドモード

【クラウドモード】スイッチは、Kaspersky Endpoint Security がライト版の定義データベースを使用する動作モードを有効または無効にします。このモードは、Kaspersky Security Network への参加が有効な場合にのみ使用可能です。ライト版の定義データベースを使用すると、コンピュータのメモリの使用量を、これ以外の場合の通常の定義データベースで使用する量の約半分にすることができます。Kaspersky Security Network に参加していない、またはクラウドモードが無効になっている場合は、カスペルスキーのサーバから完全版の定義データベースがダウンロードされます。

スイッチをオンにすると、ライト版の定義データベースが使用され、オペレーティングシステムリソースの負荷が軽減されます。

注意： ライト版の定義データベースは、チェックボックスをオンにした後の次のアップデート中にダウンロードされます。

スイッチをオフにすると、完全版の定義データベースが使用されます。

注意： 完全版の定義データベースは、チェックボックスをオフにした後の次のアップデート中にダウンロードされます。

KSN 声明

このリンクをクリックするとウインドウが開き、[Kaspersky Security Network](#) に関する声明のテキストを読み、[Kaspersky Security Network への参加条件に同意することができます](#)。

注意： Kaspersky Security Center Web コンソールを介して Kaspersky Endpoint Security を管理している場合、Kaspersky Security Center の設定に応じて、Kaspersky Security Network の代わりに Kaspersky Private Security Network への参加を行うことができます。Kaspersky Security Center Cloud コンソールを介して Kaspersky Endpoint Security を管理している場合、Kaspersky Private Security Network への参加はできません。Kaspersky Private Security Network への参加に関する詳細は、[Kaspersky Security Center のヘルプ](#)  を参照してください。

【KSN プロキシ設定】セクションでは、KSN プロキシを設定できます。

KSN プロキシを使用する

Kaspersky Security Network への接続時にプロキシサーバを使用するかどうかを選択します。

このチェックボックスをオンにすると、プロキシサーバを使用して Kaspersky Security Network に接続します。

このチェックボックスをオフにすると、Kaspersky Security Network に直接接続します。

既定では、このチェックボックスはオフです。

KSN プロキシを使用できない場合はカスペルスキーのサーバを使用する [?](#)

KSN プロキシが使用できない場合、カスペルスキーのサーバを使用するかどうかを選択します。

このチェックボックスをオンにすると、KSN プロキシが使用できない場合にカスペルスキーのサーバを使用します。

このチェックボックスをオフにすると、KSN プロキシが使用できない場合にカスペルスキーのサーバを使用しません。

既定では、このチェックボックスはオフです。

このチェックボックスは、**[KSN プロキシを使用する]** をオンにすると使用可能になります。

強制適用 [?](#)

[強制適用] スイッチをオンにすると、Kaspersky Endpoint Security は、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値の変更を禁止します。

[強制適用] スイッチをオフにすると、Kaspersky Endpoint Security では、ローカルコンピュータ上のタスク設定、アプリケーション設定、サブグループのポリシー、およびセカンダリ管理サーバーの値が変更できます。

[Kaspersky Security Network / Kaspersky Private Security Network への参加] ウィンドウ

[すべて表示](#) | [すべて隠す](#)

詳細 [?](#)

このリンクをクリックすると新しいブラウザウィンドウが開き、Kaspersky Security Network または Kaspersky Private Security Network に関する声明のテキストを読むことができます。

Kaspersky Security Network / Kaspersky Private Security Network への参加の条項に同意する [?](#)

ポリシーが適用されたコンピュータは、Kaspersky Security Network / Kaspersky Private Security Network に参加します。

Kaspersky Security Network / Kaspersky Private Security Network への参加の条項に同意しない [?](#)

ポリシーが適用されたコンピュータは、Kaspersky Security Network / Kaspersky Private Security Network に参加しません。

注意：Kaspersky Security Center Cloud コンソールを介して Kaspersky Endpoint Security を管理している場合、Kaspersky Private Security Network への参加はできません。Kaspersky Private Security Network への参加に関する詳細は、[Kaspersky Security Center のヘルプ](#) [?](#) を参照してください。

[アクセスを許可] ダイアログ

[すべて表示](#) | [すべて隠す](#)

回復キーを取得 [?](#)

このボタンをクリックすると、クライアントコンピュータ上の暗号化されたディスクにアクセスするために必要な回復キーが生成されます。

コマンドラインからの製品の管理

Kaspersky Endpoint Security は、コマンドラインから管理できます。

注意：Kaspersky Endpoint Security のモジュールのアップデートのインストール後、コマンドラインの製品のクライアントのバージョンが、インストールされた製品のバージョンとは異なっている場合があります。

コマンドラインの構文：

kav <コマンド> <パラメータ>

コマンドにはそれぞれ固有のさまざまなパラメータがあります。

コマンドラインヘルプの表示

製品のコマンドラインの構文についての情報を表示するには次のコマンドを使用します：

```
kav -? | help
```

マルウェアスキャンの実行

コマンドの構文：

```
kav scan <スキャン範囲> <処理> <ファイル種別> <除外リスト> <レポートのパラメータ> <詳細なパラメータ>
```

注意：マルウェアスキャンの実行には、本製品で作成したタスクを使用することもできます。その場合は、[タスクをコマンドラインから起動してください](#)。タスクは Kaspersky Endpoint Security のインターフェイスで指定されたパラメータを使用して実行されます。

パラメータの説明

<スキャン範囲> - 悪意のあるコードの有無をスキャンするオブジェクトのリストです。次に示す複数のパラメータを空白文字で区切って含めることができます。

注意：Kaspersky Endpoint Security は、OneDrive や iCloud ストレージ、その他のクラウドストレージにあるファイルをスキャンしません。これらのファイルをスキャン範囲から除外してください。そうしないと、スキャンタスクが「感染したファイルが削除されませんでした」というエラーで終了する可能性があります。

次の値が選択できます：

- **<ファイル>** - スキャン対象のファイルまたはフォルダの場所のリスト。ファイルへの絶対パスまたは相対パスを使用できます。リストの項目は空白文字で区切られます。

注意：オブジェクト名やオブジェクトのパスに空白や特殊な文字（\$、&、@ など）が含まれる場合には、全体を単一引用符で囲むか、除外する文字の左側にバックスラッシュを挿入してエスケープしてください。特定のフォルダが指定された場合、そのフォルダのすべてのファイルとフォルダがスキャンされます。

- **-all** - コンピュータの完全スキャン。
- **-remdrives** - すべてのリムーバブルドライブ。
- **-fixdrives** - すべての内部ディスク。
- **-netdrives** - すべてのネットワークドライブ。
- **-@:<Filelist.lst>** - スキャン範囲内のオブジェクトおよびフォルダのリストを含むファイルのパスファイルはテキスト形式で、各スキャンオブジェクトは別々の行に記載されている必要があります。ファイルへの絶対パスのみを入力できます。

<処理> - スキャン中に検知された悪意のあるオブジェクトの処理方法を決定します。このパラメータが指定されていない場合は、値 **-i8** の処理が既定で実行されます。

次の値が選択できます：

- **-i0** - オブジェクトの情報をレポートに保存します。オブジェクトに対する処理は実行しません。
- **-i1** - 感染したオブジェクトを駆除し、駆除できない場合はスキップします。
- **-i2** - 感染したオブジェクトを駆除し、駆除できない場合は削除します。実行ヘッダがあるコンテナ（sfx 圧縮ファイル）以外のコンテナは削除しません。
- **-i3** - 感染したオブジェクトを駆除し、駆除できない場合は削除します。コンテナ内の感染したファイルを削除できない場合は、コンテナを完全に削除します。
- **-i4** - 感染したオブジェクトを削除します。削除できない感染したファイルがコンテナの内部にある場合は、コンテナを完全に削除します。
- **-i8** - 感染したオブジェクトを検知した場合、ユーザに処理を確認します（既定で使用されます）。

- **-i9** - スキャンの完了時にユーザに処理を確認します。

<ファイル形式> - マルウェアスキャンの対象となるファイル形式を指定します。このパラメータが指定されていない場合、既定では、感染の可能性があるファイルのみを、ファイルの内容に基づいてスキャンします。

次の値が選択できます：

- **-fe** - 感染の可能性があるオブジェクトのみを、ファイルの拡張子に基づいてスキャンします。
- **-fi** - 感染の可能性があるファイルのみを、ファイルの内容に基づいてスキャンします。既定では、このパラメータが使用されています。
- **-fa** - すべてのファイルをスキャンします。

<除外> - スキャンから除外するオブジェクトを指定します。次に示す複数のパラメータを空白文字で区切って含めることができます。

次の値が選択できます：

- **-e:a** - 圧縮ファイルをスキャンしません。
- **-e:b** - メールデータベースをスキャンしません。
- **-e:m** - テキスト形式のメールをスキャンしません。
- **-e:<mask>** - マスクを基準としてオブジェクトをスキャンしません。
- **-e:<秒>** - 指定された時間（秒単位）よりも長くスキャンされているオブジェクトをスキップします。
- **-es:<サイズ>** - 指定された値（メガバイト単位）より大きいサイズのオブジェクトをスキップします。

<レポートのパラメータ> - スキャン結果のレポート形式を決定します。レポートへの絶対パスまたは相対パスを使用できます。このパラメータが指定されていない場合、スキャン結果とすべてのイベントが表示されます。

次の値が選択できます：

- **-r:<レポートファイル>** - 重要なイベントのみを指定されたレポートファイルに記録します。
- **-ra:<レポートファイル>** - すべてのイベントを指定されたレポートファイルに記録します。

<詳細なパラメータ> - スキャン技術の使用と設定情報ファイルの使用設定を定義するパラメータ：

- **-iSwift=<on|off>** - iSwift の使用を有効または無効にします。
- **-c:<設定情報ファイル>** - マルウェアスキャンで使用するアプリケーション設定を含む設定情報ファイルのパスを定義します。ファイルへの絶対パスまたは相対パスを使用できます。このパラメータが指定されていない場合、コマンドラインで既に指定されている値とともに、インターフェイスで設定された値が使用されます。

例：

フォルダ ~/Documents、/Applications、およびファイル my test.exe のスキャンを開始します：

```
kav scan ~/Documents /Applications 'my test.exe'
```

ファイル object2scan.txt に登録されているオブジェクトをスキャンします。設定情報ファイル scan_settings.txt を使用します。スキャンの完了時に、すべてのイベントを記録するレポートを作成します：

```
kav scan -@:objects2scan.txt -c:scan_settings.txt -ra:scan.log
```

設定情報ファイルのサンプル：

```
-netdrives -@:objects2scan.txt -ra:scan.log
```

製品のアップデート

コマンドの構文：

```
kav update <アップデート元> <レポートのパラメータ> <詳細なパラメータ>
```

パラメータの説明

<アップデート元> - アップデートのダウンロード元となる HTTP サーバ、ネットワークフォルダ、またはローカルフォルダ。パスが選択されていない場合、アップデート元は本製品のアップデート設定から取得されます。

<レポートのパラメータ> - スキャン結果のレポート形式を決定します。レポートへの絶対パスまたは相対パスを使用できます。このパラメータが指定されていない場合、アップデート結果とすべてのイベントが表示されます。

次の値が選択できます：

- **-r:<レポートファイル>** - 重要なイベントのみを指定されたレポートファイルに記録します。
- **-ra:<レポートファイル>** - すべてのイベントを指定されたレポートファイルに記録します。

<詳細なパラメータ> - 設定情報ファイルの使用法を指定します。

-c:<設定情報ファイル> - 本製品のアップデート時に使用するアプリケーション設定を含む設定情報ファイルのパスを定義します。ファイルへの絶対パスまたは相対パスを使用できます。このパラメータが定義されていない場合、インターフェイスで設定された値が使用されます。

例：

既定のアップデート元から定義データベースをアップデートします。すべてのイベントがレポートに記録されます：

```
kav update -ra:avbases_upd.txt
```

設定情報ファイル updateapp.ini のパラメータを使用して Kaspersky Endpoint Security のモジュールをアップデートします：

```
kav update -app=on -c:updateapp.ini
```

前回のアップデートのロールバック

コマンドの構文：

```
kav rollback <レポートのパラメータ>
```

重要：このコマンドの実行には管理者権限が必要です。

パラメータの説明

<レポートのパラメータ> - アップデートのロールバック結果のレポートの形式を指定します。レポートへの絶対パスまたは相対パスを使用できます。このパラメータが指定されていない場合、ロールバック結果とすべてのイベントが表示されます。

次の値が選択できます：

- **-r:<レポートファイル>** - 重要なイベントのみを指定されたレポートファイルに記録します。
- **-ra:<レポートファイル>** - すべてのイベントを指定されたレポートファイルに記録します。

例：

```
kav rollback -ra:rollback.txt
```

コンポーネントまたはタスクの開始と停止

start コマンドの構文：

```
kav start <タスクまたはコンポーネントの名前> <レポートのパラメータ>
```

stop コマンドの構文：

```
kav stop <タスクまたはコンポーネントの名前>
```

重要：停止コマンドの実行には管理者権限が必要です。

パラメータの説明

<タスクまたはコンポーネントの名前> - 次のいずれかの値を指定します：

- **fm** または **file_monitoring** - ファイル脅威対策

- **wm** または **web_monitoring** - ウェブ脅威対策
- **ids** - ネットワーク脅威対策
- **full** または **scan_my_computer** - 完全スキャンタスク
- **scan_objects** - オブジェクトスキャンタスク
- **quick** または **scan_critical_areas** - 簡易スキャンタスク
- **updater** - アップデートタスク
- **rollback** - ロールバックタスク

<レポートのパラメータ> - コンポーネントまたはタスクの結果のレポート形式を決定します。レポートへの絶対パスまたは相対パスを使用できます。このパラメータが定義されていない場合、インターフェイスで設定されたパラメータに従って結果を表示します。

注意： <レポートのパラメータ> は、**scan_objects**、**updater**、および **rollback** の値でのみ使用できます。

次の値が選択できます：

- **-r:<レポートファイル>** - 重要なイベントのみを指定されたレポートファイルに記録します。
- **-ra:<レポートファイル>** - すべてのイベントを指定されたレポートファイルに記録します。

注意： コマンドプロンプトから開始されるコンポーネントおよびタスクは、インターフェイスで設定されたパラメータを使用して実行されません。

例：

ファイル脅威対策を有効にするには、コマンドラインに次のコマンドを入力します：

```
kav start fm
```

コマンドラインから完全スキャンを停止するには、次のコマンドを入力します：

```
kav stop scan_my_computer
```

コンポーネントまたはタスクのステータスと統計の表示

status コマンドの構文：

```
kav status <タスクまたはコンポーネントの名前>
```

statistics コマンドの構文：

```
kav statistics <タスクまたはコンポーネントの名前>
```

パラメータの説明

<タスクまたはコンポーネントの名前> - 次のいずれかの値を指定します：

- **fm** または **file_monitoring** - ファイル脅威対策
- **wm** または **web_monitoring** - ウェブ脅威対策
- **mail_monitoring** - メール脅威対策
- **ids** - ネットワーク脅威対策
- **firewall** - ファイアウォール
- **behaviordetection** - ふるまい検知
- **exploitprevention** - 脆弱性攻撃ブロック
- **remediationengine** - 修復エンジン

- **devicecontrol** – デバイスコントロール
- **webcontrol** – ウェブコントロール
- **full** または **scan_my_computer** – 完全スキャンタスク
- **scan_objects** – オブジェクトスキャンタスク
- **quick** または **scan_critical_areas** – 簡易スキャンタスク
- **externalstoragesscanner** – リムーバブルドライブスキャンタスク
- **updater** – アップデートタスク
- **rollback** – ロールバックタスク
- **diskencryption** – FileVault ディスク暗号化の設定
- **edroptimum** – Endpoint Detection and Response Optimum
- **edrkata** – Endpoint Detection and Response (KATA)
- **cloudsandbox** – Cloud Sandbox
- **mdr** – Managed Detection and Response

注意： <タスクまたはコンポーネントの名前> の値を指定せずに **status** コマンドを実行すると、製品のすべてのタスクとコンポーネントの現在の状態が表示されます。 **statistics** コマンドの場合、パラメータ <タスクまたはコンポーネントの名前> に値を指定する必要があります。

保護設定のエクスポート

コマンドの構文：

```
kav export <タスクまたはコンポーネントの名前> <エクスポートファイル>
```

パラメータの説明

<タスクまたはコンポーネントの名前> - 次のいずれかの値を指定します：

- **fm** または **file_monitoring** – ファイル脅威対策
- **wm** または **web_monitoring** – ウェブ脅威対策
- **ids** – ネットワーク脅威対策
- **full** または **scan_my_computer** – 完全スキャンタスク
- **scan_objects** – オブジェクトスキャンタスク
- **quick** または **scan_critical_areas** – 簡易スキャンタスク
- **updater** – アップデートタスク
- **rollback** – ロールバックタスク

<エクスポートファイル> - 本製品の設定のエクスポート先ファイルのパス。ファイルへの絶対パスまたは相対パスを使用できます。

例：

```
kav export fm fm_settings.txt
```

本製品のアクティベーション

ライセンス情報ファイルを適用して Kaspersky Endpoint Security をアクティベートできます。

コマンドの構文：

```
kav license /add <ライセンス情報ファイルまたはライセンスのアクティベーションコード>
```

パラメータの説明

<ライセンス情報ファイル> - 拡張子がKEY のライセンス情報ファイル。

<ライセンスアクティベーションコード> - XXXX-XXXX-XXXX-XXXX 形式のアクティベーションコード。

例：

```
kav license /add ./1AA111A1.key
kav license /add A11A1-11111-1A1AA-1A11A
```

システム機能拡張のインストール

コマンドの構文：

```
kav activatesystemextension /sysext
```

注意：Kaspersky Endpoint Security のネットワークコンテンツのフィルタ機能の権限を [プライバシーとセキュリティ] 設定で許可し、設定を終了する必要があります。

ネットワーク接続の設定

ウェブ脅威対策、ネットワーク脅威対策のためのネットワーク接続を設定できます。

コマンドの構文：

```
kav activatesystemextension /webav
```

注意：Kaspersky Endpoint Security のネットワークコンテンツのフィルタ機能の権限を許可し、設定を終了する必要があります。

ライセンス情報の削除

本製品に現在追加済みであるライセンス情報をすべて削除できます。

コマンドの構文：

```
kav license /del
```

重要：このコマンドの実行には管理者権限が必要です。

コマンドラインのリターンコード

コマンドラインでは、コマンドから一般的なコードが返される場合があります。リターンコードには一般的なコードと、ある特定のタスクに固有のコードがあります。

リターンコードを受け取るためのコマンドの構文：

```
echo $?
```

一般的なリターンコード：

- 0 - 操作が正常に完了しました
- 1 - パラメータの値が無効です
- 2 - 不明なエラー
- 3 - タスクの完了エラーです
- 4 - タスクがキャンセルされました

マルウェアスキャンのリターンコード：

- 101 - 悪意のあるオブジェクトがすべて処理されました

- 102 - 悪意のあるオブジェクトが検知されました

本製品の終了

コマンドの構文：

```
kav exit
```

重要：このコマンドの実行には管理者権限が必要です。

本製品のアンインストール

Kaspersky Endpoint Security をコマンドラインから削除するには、次のコマンドシーケンスを使用します：

```
sudo /Library/Application\ Support/Kaspersky\ Lab/klnagent/Binaries/UninstallScript
sudo /Library/Application\ Support/Kaspersky\ Lab/KAV/Binaries/UninstallScript
sudo rm -rf /Library/Application\ Support/Kaspersky\ Lab/ /Applications/Kaspersky
```

重要：本製品のアンインストールには、管理者権限が必要です。

Detection and Response 管理コマンド

コマンドラインを使用して、Detection and Response ソリューションのビルトイン機能を管理できます。Kaspersky Security Center コンソールを使用した管理が不可能な場合は、Detection and Response を管理できます。

実行防止の管理

クライアントコンピューターの実行防止設定を表示し、クライアントコンピューターの実行防止を無効にすることができます。

コマンドの構文：

```
kav prevention </disable | /show>
```

コマンドの説明

/disable - クライアントコンピューター上の実行防止をオフにするコマンド。

/show - モードや実行防止ルールの一覧など、現在の実行防止設定を表示するコマンド。

ネットワーク分離の管理

ホストのネットワーク分離設定を表示し、ホスト上のネットワーク分離を無効にすることができます。

コマンドの構文：

```
kav isolation </off | /status>
```

コマンドの説明

/off - ネットワーク分離をオフにするコマンド。

重要：このコマンドの実行には管理者権限が必要です。

/status - ネットワーク分離ステータスと除外を表示するコマンド。

注意：これらのコマンドは同時に実行する必要があります。

テクニカルサポートへの問い合わせ

このセクションでは、テクニカルサポートを受ける方法と、テクニカルサポートの利用条件について説明します。

テクニカルサポートのご利用方法

本製品のヘルプや任意の情報源で問題の解決策が見つからない場合は、カスペルスキーのテクニカルサポートまでお問い合わせください。テクニカルサポートの担当者が製品のインストールや使用に関する質問に回答します。

注意：カスペルスキーによる本製品のサポートは、本製品のライフサイクル期間中に提供されます（[製品のサポートライフサイクルページ](#)を参照）。テクニカルサポートに連絡する前に、[サポートサービス規約](#)をお読みください。

テクニカルサポートへの連絡方法は次の通りです：

- [テクニカルサポートサイトを参照する](#)
- [Kaspersky Company Account ポータル](#) から、テクニカルサポートへリクエストを送信する

カスペルスキーカンパニーアカウントによるテクニカルサポート

[カスペルスキーカンパニーアカウント](#) は、カスペルスキー製品を使用する企業向けのポータルです。このポータルは、オンラインリクエストを通じてユーザとカスペルスキーのエキスパートの交流を促進するよう設計されています。また、オンラインリクエストのステータスを追跡したり、オンラインリクエストの履歴を保存することもできます。

カスペルスキーカンパニーアカウントでは、シングルアカウントで組織の全従業員を登録できます。シングルアカウントによって、登録従業員からカスペルスキーまでのオンラインリクエストを一元管理でき、カスペルスキーカンパニーアカウントを介して従業員の権限を管理することもできます。

カスペルスキーカンパニーアカウントのポータルは、次の言語で利用できます：

- 英語
- スペイン語
- イタリア語
- ドイツ語
- ポーランド語
- ポルトガル語
- ロシア語
- フランス語
- 日本語

カスペルスキーカンパニーアカウントの詳細は、[テクニカルサポートサイト](#)を参照してください。

テクニカルサポート用の情報収集

サポートとトラブルシューティングの効率向上のため、テクニカルサポートでは診断中にデバッグ目的で一時的に設定の変更を依頼することがあります。それには次の操作が必要になることがあります：

- 拡張診断情報を収集する機能をオンにします。
- 標準ユーザインターフェイスからは使用できない、個々の製品コンポーネントの設定を微調整します。
- 収集した診断情報の送信に関する設定を変更します。

テクニカルサポート担当者は、リストされた操作の実行に必要なすべての情報を提供し、デバッグ目的で収集するデータの範囲について説明します。拡張診断情報が収集された後、その情報はユーザのコンピュータに保存されます。収集したデータは自動的にカスペルスキーに送信されません。

トレースファイルの使用

テクニカルサポート担当者への問題の報告後、動作に関する情報を含むレポートを生成し、テクニカルサポートへ送信するように依頼される場合があります。その場合、[トレースファイル](#)の作成も依頼される場合があります。トレースファイルによって、アプリケーションコマンドの実行を順を追って調査し、エラーが発生したコマンドを特定できます。

トレースファイルの作成

追跡は、アプリケーション活動の詳細情報を記録する効果的な手段です。テクニカルサポートでは、問題の解決にトレースファイルを使用します。

[トレースファイルの作成](#)

1. メニューバーで製品アイコンをクリックし、**〔設定〕** を選択します。
本製品の設定ウインドウが表示されます。
2. **〔インターフェイス〕** タブの **〔トレース〕** セクションで、**〔トレースを有効にする〕** をオンにします。

重要：テクニカルサポートから指示された場合にのみ、トレースを有効にしてください。

トレースファイルは、ハードディスクの容量を大量に使用することがあります。トレースファイルが不要になった場合は、トレースを無効にしてください。

トレースを無効にする

1. メニューバーで製品アイコンをクリックし、**〔設定〕** を選択します。
本製品の設定ウインドウが表示されます。
2. **〔インターフェイス〕** タブの **〔トレース〕** セクションで、**〔トレースを有効にする〕** をオフにします。

トレースファイルには、次の情報が保存されます：

- 端末とオペレーティングシステムに関する情報（デバイスの一意な識別子、デバイスの種別、ネットワークデバイスの **MAC** アドレス、オペレーティングシステムの種別、オペレーティングシステムのバージョン）。
- 本製品および本製品のモジュールの動作に関する情報。
- 定額制サービスに関する情報（定額制サービスの種別、地域）。
- 言語、アプリケーションの識別子、アプリケーションのカスタマイズ、アプリケーションのバージョン、アプリケーションのインストールの一意な識別子、端末の一意な識別子に関する情報。
- マルウェア対策による端末の保護の状態、処理または検知されたすべてのオブジェクトおよびその対処（検知されたオブジェクトの名前、検知日時、ダウンロード元の **URL**、感染したファイルの名前とサイズ、それらのファイルのパス、攻撃元コンピュータの **IP** アドレスとネットワーク攻撃の標的になったポートの番号、マルウェアによる活動のリスト、望ましくない **URL**）、製品およびユーザーによる関連する操作および決定。
- ユーザーがダウンロードしたアプリケーションに関する情報（**URL**、属性、ファイルサイズ、ダウンロードプロセスに関する情報）。
- 起動したアプリケーションおよびそのモジュールに関する情報（サイズ、属性、作成日、**PE** ヘッダーの詳細、地域、製品名、場所、パッケージ）。
- インストールされているカスペルスキー製品のインターフェイスのエラーや使用に関する情報。
- ネットワーク接続に関する情報：リモートコンピュータおよびユーザーのコンピュータの **IP** アドレス、接続に使用されたポート番号、接続のネットワークプロトコル。
- **IT** および通信ネットワークを介してコンピュータから送受信されたネットワークパケットに関する情報。
- 送受信されたメールおよびインスタントメッセージに関する情報。
- アクセスされた **URL** に関する情報：オープンなプロトコルを使用して接続が確立された時間、**Web** サイトのログインおよびパスワードに関する情報、**Cookie** の内容。
- サーバの公開証明書。

トレースファイルには、本製品の修正に必要な情報のみが含まれます。カスペルスキーは、**Kaspersky Endpoint Security** の動作中に発生したエラーと関係があるインシデントを調査するため、トレースファイルを使用します。

既定では、トレースファイルの作成は無効になっています。トレースファイルの作成は、本製品の設定で有効にできます。

トレースファイルのカスペルスキーへの送信は、手動でのみ可能です。本製品が自動的にトレースファイルをカスペルスキーに送信することはありません。

トレースファイルのカスペルスキーへの送信方法を選択できます。

カスペルスキーへトレースファイルを送信する前に、含まれるデータを確認してください。

重要：トレースファイルには、個人情報または機密情報が含まれる可能性があります。カスペルスキーヘトレースファイルを送信することで、送信したトレースファイル内のすべての情報をカスペルスキーに提供することに同意し、送信時に使用された方法にも同意したことになります。

製品の情報源

カスペルスキーの Web サイトの [Kaspersky Endpoint Security](#) のページ

[カスペルスキーの Web サイトの Kaspersky Endpoint Security に関するページ](#) では、製品やその機能および特徴に関する一般的な情報を確認できます。

ナレッジベースの [Kaspersky Endpoint Security](#) のページ

ナレッジベースは、カスペルスキーのテクニカルサポートサイトのセクションの1つです。

[ナレッジベースの Kaspersky Endpoint Security のページ](#) に、製品の購入、インストール、使用の方法について、役立つ情報、推奨事項、および FAQ への回答が掲載されています。

記事では、本製品だけではなく他のカスペルスキー製品に関連した質問にも回答しています。ナレッジベースの記事には、カスペルスキーのテクニカルサポートからのお知らせも含まれる場合があります。

[ヘルプのメニューからナレッジベースへアクセス](#)

1. [ヘルプ] → [サポート] の順に選択します。
2. テクニカルサポートをクリックします。

Web フォーラムの利用

即答を必要としない質問については、[Web フォーラムで](#) カスペルスキーのエキスパートや他のユーザとディスカッションできます。

フォーラムでは、ディスカッションのトピックの表示、コメントの投稿、新しいトピックの作成ができます。

[ヘルプのメニューからフォーラムへアクセス](#)

1. [ヘルプ] → [サポート] の順に選択します。
2. [コミュニティ] をクリックします。

注意：Web サイトへのアクセスには、インターネット接続が必要です。

問題の解決方法が見つからない場合は、[カスペルスキーのテクニカルサポートへお問い合わせください](#)。

本製品のヘルプ

本製品には、フルヘルプとコンテキストヘルプが含まれています。

フルヘルプは、[Kaspersky Endpoint Security](#) の設定方法および使用方法に関する情報を提供します。

コンテキストヘルプでは、[Kaspersky Endpoint Security](#) のウインドウや設定に関する情報を提供しています。また、それらの設定を使用するタスクの説明へのリンクも含まれています。

ヘルプは、配布キットに含まれるか、カスペルスキーの Web サイトで確認できます。オンラインヘルプを確認するには、インターネットに接続する必要があります。

オンラインヘルプ（このヘルプ）

このヘルプでは、次の情報を確認できます：

- 本製品のインストール準備、本製品のインストールとアクティベーション。
- 本製品の設定と使用。
- Kaspersky Security Center を使用した本製品のリモート管理。

付録

このセクションでは、本文を補足する情報を提供します。

既知の問題と制限

Kaspersky Endpoint Security には、次の問題と制限があります：

- 情報を収集し、処理する目的でその情報を送信するアプリケーションがコンピュータにインストールされている場合、そのアプリケーションは Kaspersky Endpoint Security によってマルウェアに分類されることがあります。これを防ぐには、このガイドの説明に従って Kaspersky Endpoint Security を設定して、該当するアプリケーションをスキャン対象から除外してください。
- 本製品の機能設定は、設定情報ファイルを編集することで変更できます。
- Kaspersky Security Center で、管理対象デバイスのプロパティにローカルタスクが重複して表示される場合があります。
- ローカルのアップデートタスクのアップデート元を変更すると、アップデートタスクが自動的に実行できなくなります。
- ユーザ宛てのセミコロン (;) を含むメッセージを設定したコンピュータの再起動タスクを管理コンソールを使用して開始すると、タスクは完了したと表示されますが、ユーザーには Mac の再起動が要求されません。
- Safari のネットワークトラフィックを本製品のスキャンから除外するには、次のパスを除外リストに追加する必要があります：
 - /System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.Networking.xpc/Contents/MacOS
 - /System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.WebContent.xpc/Contents/MacOS
 - /System/Library/PrivateFrameworks/SafariShared.framework/Versions/A/XPCServices/com.apple.Safari.SearchHelper.xpc
 - /System/Library/Frameworks/webkit2.framework/versions/a/xpcservices/com.apple.webkit.networking.xpc/contents/macc
- Google Chrome のネットワークトラフィックをスキャンから除外するには、次のパスを除外リストに追加する必要があります：
 - /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/<バージョン番号>/Helpers/Google Chrome Helper.app/Contents/MacOS/Google Chrome Helper
- Kaspersky Security Center Web コンソールと Cloud コンソールを使用して Kaspersky Endpoint Security ポリシーのポリシープロファイルを作成した後、設定がクライアントコンピュータに正しく適用されていることを確認する必要があります。
- FileVault ディスク暗号化をポリシーの設定で有効にすると、管理者権限を持つユーザがシステム設定から Mac の起動ディスクを復号化できるようになります。
- プロキシサーバのオプション変更は、本製品を再起動しないと適用されません。
- 信頼されない証明書を持つ Web サイトに Safari が接続できない場合があります。その場合、その Web サイトを除外リストに追加するか、別のブラウザを使用してください。
- Kaspersky Security Center を使用して Kaspersky Endpoint Security 11.2 以降をリモートでアンインストールすると、本製品の機能拡張がコンピュータのメモリに残る場合があります。この後、まれに、Kaspersky Endpoint Security のインストール時にフルディスクアクセスの許可に関する問題が発生する場合があります。この場合、ローカルで本製品をアンインストールし、再インストールすることを推奨します。
- Rosetta を必要とするアプリケーションが、Kaspersky Endpoint Security が実行されているとインストールされない場合があります。この問題を解決するには、Kaspersky Endpoint Security を終了し、アプリケーションの再インストールを試行してください。
- 複合オブジェクト内で検知された脅威のアラートの詳細には、脅威開発チェーンのグラフはなく、検知されたオブジェクト自体に関する情報のみが含まれます。
- パスワードによる保護のためにパスワードを保存する時にエラーが発生する場合があります。この場合、本製品をアンインストールして再インストールすることを推奨します。
- Kaspersky Endpoint Security は、OneDrive や iCloud ストレージ、その他のクラウドストレージにあるファイルをスキャンしません。これらのファイルをスキャン範囲から除外してください。そうしないと、スキャンタスクが「感染したファイルが削除されませんでした」というエラーで終了する可能性があります。
- [ファイルの隔離] タスクの結果として隔離されたオブジェクトはスキャンできません。
- Kaspersky Security Center では、NetBIOS 名、コンピュータ名、ホスト名が同じ場合にのみデバイス名が正しく表示されます。

拡張子に応じてスキャンされるオブジェクトのリスト

スキャンタスクの環境設定で「**アプリケーションとドキュメントをスキャン（拡張子で判断）**」を選択した場合は、拡張子のないオブジェクトと次の拡張子のオブジェクトがマルウェアスキャンの対象になります：

一般的な形式：

- txt
- csv
- htm
- html

マルチメディア（オーディオ / ビデオ）ファイル：

- flv
- f4v
- avi
- 3gp
- 3g2
- 3gp2
- 3p2
- divx
- mp4
- mkv
- mov
- qt
- asf
- wmv
- rm
- rmvb
- vob
- dat
- mpg
- mpeg
- bik
- fcs
- mp3
- mpeg3
- flac
- ape
- ogg
- aac

- m4a
- wma
- ac3
- wav
- mka
- rm
- ra
- ravb
- mid
- midi
- cda

画像ファイル：

- jpg
- jpe
- jpeg
- jff
- gif
- png
- bmp
- tif
- tiff
- emf
- wmf
- eps
- psd
- cdr
- swf

実行ファイルとシステムファイル：

- exe
- dll
- scr
- ocx
- com
- sys
- class
- o

- so
- elf
- prx
- vb
- vbs
- js
- bat
- cmd
- msi
- deb
- rpm
- sh
- pl
- dylib

ドキュメントとテンプレート：

- doc
- dot
- docx
- dotx
- docm
- dotm
- xsl
- xls
- xlsx
- xltx
- xlsm
- xltm
- xlam
- xlsb
- ppt
- pot
- pps
- pptx
- potx
- pptm
- potm
- ppsx

- ppsm
- rtf
- pdf
- msg
- eml
- vsd
- vss
- vst
- vdx
- vsx
- vtx
- xps
- oxps
- one
- onepkg
- xsn
- odt
- ods
- odp
- sxw
- pub
- mdb
- accdb
- accde
- accdr
- accdc
- chm
- mht

圧縮ファイル：

- zip
- 7z*
- 7-z
- rar
- iso
- cab
- jar
- bz

- bz2
- tbz
- tbz2
- gz
- tgz
- arj
- dmg
- smi
- img
- xar

注意：実際のファイル形式は、そのファイル名の拡張子と一致しないことがあります。

ファイルおよびフォルダへのパスのマスク

ファイル名のマスクまたはフォルダ名のマスクは、ファイルの名前と拡張子、またはフォルダ名を、共通の記号で表記します。

これらの記号は、保護範囲、スキャン範囲、および信頼ゾーンを指定する時に使用できます：

- チルダ記号（~）は、ファイルまたはフォルダへのパスにある `/Users/<ユーザ名>` を置換します。たとえば、`~/Desktop` というパスは、保護対象コンピュータのすべてのユーザのデスクトップフォルダが保護範囲に含まれることを意味します。
- アスタリスク記号（*）は、ファイル名またはフォルダ名の任意の文字セットとして使用できます（「\」と「/」（ファイルまたはフォルダへのパスにあるファイル名またはフォルダ名の区切り文字として使用）は除きます）。たとえば、「`/*/*.txt`」は、内部ディスク内のフォルダにある拡張子 `TXT` のファイルへのパスをすべて含みますが、サブフォルダ内のファイルは含みません。
- 2文字の連続したアスタリスク記号（**）は、ファイル名またはフォルダ名の任意の文字（空白のセットも含む）として使用できます。「\」と「/」（ファイルまたはフォルダへのパスにあるファイル名またはフォルダ名の区切り文字として使用）も含まれます。たとえば、「`/Folder/**/*.txt`」は、**C:** ドライブ内のフォルダ「`Folder`」とそのサブフォルダにある拡張子 `TXT` のファイルへのパスをすべて含みます。マスクには、少なくとも1つのネストレベルを含む必要があります。「`/**/*.txt`」は、有効なマスクではありません。
- 疑問符（?）は、ファイル名またはフォルダ名の任意の1文字として使用できます（「\」と「/」（ファイルまたはフォルダへのパスにあるファイル名またはフォルダ名の区切り文字として使用）は除きます）。たとえば、「`/Folder/???.txt`」は、**C:** ドライブ内のフォルダ「`Folder`」とそのサブフォルダにあり、名前が3文字である拡張子 `TXT` のファイルへのパスをすべて含みます。

IOC ファイルの要件

IOC スキャンタスクを作成する時は、次の[IOC ファイルの ?](#)要件と制限を考慮してください：

- 本製品は、セキュリティ侵害インジケータを記述するためのオープン標準 **OpenIOC** バージョン **1.0** および **1.1** または **STIX** バージョン **2.0** および **2.1** の **IOC**、**XML** および **JSON** 拡張子を持つ **IOC** ファイルをサポートします。
- コマンドラインで **IOC** スキャンタスクを作成する時に、サポートされていない **IOC** ファイルをアップロードすると、タスクの実行時に、サポートされている **IOC** ファイルのみが使用されます。コマンドラインで **IOC** スキャンタスクを作成する時に、アップロードしたすべての **IOC** ファイルがサポートされていないことが判明した場合もタスクは実行できますが、セキュリティ侵害インジケータは検知されません。**Web** コンソールまたは **Cloud** コンソールを使用して、サポートされていない **IOC** ファイルをアップロードすることはできません。
- **IOC** ファイル内のセマンティックエラーやサポートされていない **IOC** 用語およびタグによって、タスクの実行が失敗することはありません。**IOC** ファイルのこのようなセクションでは、本製品は一致を検知しません。
- 単一の **IOC** スキャンタスクで使用するすべての **IOC** ファイルの識別子は一意である必要があります。同じ識別子を持つ **IOC** ファイルが存在する場合、タスクの実行結果に影響する可能性があります。
- 1つの **IOC** ファイルのサイズは **2 MB** 以内にする必要があります。サイズを超えたファイルを使用すると、**IOC** スキャンタスクがエラーで終了します。**IOC** コレクションに追加されるすべてのファイルの合計サイズは **10 MB** 以内にする必要があります。すべてのファイルの合計サイズが **10 MB** を超える場合は、**IOC** コレクションを分割し、複数の **IOC** スキャンタスクを作成する必要があります。
- 脅威ごとに1つの **IOC** ファイルを作成することを推奨します。これにより、**IOC** スキャンタスクの結果の分析が容易になります。

本製品による **IOC** ファイルのサポートの機能と制限を次のテーブルに示します。

IOC ドキュメントのサポートの機能と制限。

サポートされている条件	OpenIOC 1.0 : is isnot (集合からの例外として) contains containsnot (セットからの例外として) OpenIOC 1.1 : is contains starts-with ends-with matches greater-than less-than STIX 2.0 および 2.1 : = != > < => <= in like matches
サポートされている条件属性	OpenIOC 1.1 : preserve-case negate
サポートされている演算子	AND OR
サポートされているデータ型	"date": 日付 (適用可能な条件: is、greater-than、less-than) "int": 整数 (適用可能な条件: is、greater-than、less-than) "string": 文字列 (適用可能な条件: is、contains、matches、starts-with、ends-with) "duration": 秒単位の継続時間 (適用可能な条件: is、greater-than、less-than)
データ型解釈の特徴	「ブール文字列」「制限付き文字列」「md5」「IP」「sha256」「base64Binary」データ型は、文字列として解釈されます。 本製品は、時間間隔の形式で設定されている場合に、int および date データ型のコンテンツ設定の解釈をサポートします。 OpenIOC 1.0 : [Content] フィールドで T0 演算子を使用する: <Content type="int">49600 T0 50700</Content> <Content type="date">2009-04-28T10:00:00Z T0 2009-04-28T16:00:00Z</Content>

<Content type="int">[154192 TO 154192]</Content>

OpenIOC 11 :

greater-than と **less-than** 条件の使用

[Content] フィールドで **TO** 演算子を使用する

本製品は、インジケータが **ISO 8601**、**Zulu タイムゾーン**、**UTC 形式** で設定されている場合、**日付** と **期間** のデータ型の解釈をサポートします。

実行防止用にサポートされているスクリプトインタープリタの実行を設定

実行防止では、次のスクリプトインタープリタがサポートされています：

- PkgUtil
- PkgInstaller
- /usr/bin/osascript
- /usr/bin/osacompile
- /usr/local/bin/python
- /usr/local/bin/python3
- /usr/bin/perl
- /usr/bin/ruby
- /bin/bash
- /bin/zsh
- /bin/sh
- /bin/dash
- /bin/csh
- /bin/ksh
- /bin/tcsh

重要：実行防止ルールで指定されたスクリプトが、既に開始されている **PkgUtil** または **PkgInstaller** スクリプトインタープリターによって開かれた場合、このスクリプトの実行はブロックされません。

Kaspersky Endpoint Security の証明書を Mozilla Firefox 証明書ストアに追加する方法

ブラウザが **Mozilla Firefox** 証明書ストアを使用している場合は、カスペルスキーの証明書をエクスポートして、この証明書ストアに手動で追加する必要があります。そうしないと、ブラウザは **HTTPS** ページを表示できなくなります。

[カスペルスキーの証明書をエクスポートする](#)

1. Mac で [Launchpad] → [その他] → [キーチェーンアクセス] を開きます。
2. ウィンドウの左側のペインで [システム] をクリックし、[証明書] タブを開きます。
3. 証明書のリストで、「Kaspersky Web Anti-Virus Certification Authority」を見つけます。
4. この証明書を右クリックし、["Kaspersky Web Anti-Virus Certification Authority"を書き出す] を選択します。
5. 証明書を保存する場所を選択し、[保存] をクリックします。

カスペルスキーの証明書が保存されます。

[カスペルスキーの証明書を Mozilla Firefox 証明書ストアに追加します。](#)

1. Mozilla Firefox を開く
2. 右上隅にあるメニューボタンをクリックし、**〔設定〕** を選択します。
3. ウィンドウの左側のペインで、**〔プライバシーとセキュリティ〕** を選択します。
4. **〔証明書〕** セクションまで下にスクロールします。
5. **〔証明書の表示〕** をクリックします。
6. 表示されたウィンドウで、**〔インポート〕** をクリックします。
7. カスペルスキーの証明書ファイルを選択し、**〔開く〕** をクリックします。
8. **〔このCAを信頼してWebサイトを識別する〕** および **〔このCAを信頼してメールユーザーを識別する〕** をオンにします。**〔OK〕** をクリックします。
カスペルスキーの証明書が Mozilla Firefox 証明書ストアにインポートされます。これは、**〔証明書マネージャー〕** ウィンドウの証明書のリストに表示されます。

重要：Kaspersky Endpoint Security を再インストールするたびに、新しいカスペルスキーのルート証明書が生成されます。つまり、Kaspersky Endpoint Security 製品を再インストールするたびに、この手順を完了する必要があります。

サードパーティ製のコードに関する情報

サードパーティ製のコードに関する情報は、インストールフォルダ内のファイル **legal_notices.txt** に記載されています。

商標に関する通知

登録商標とサービスマークに関する権利は各所有者に帰属します。

App Store、Apple、Apple Remote Desktop、FileVault、iCloud、Keychain、Launchpad、Mac、Mac Pro、macOS、Rosetta、Safari、Xcode は、米国およびその他の国における Apple Inc. の商標です。

IOSは、米国およびその他の国における Cisco Systems, Inc. およびその子会社の登録商標または商標です。

Android、Chrome、Chromium、Google、Google Chrome は、Google LLC. の商標です。

Intel は、Intel Corporation またはその子会社の商標です。

Linux は米国およびその他の国における Linus Torvalds の登録商標です。

Excel、IIS、Internet Explorer、Microsoft、Microsoft Edge、Windows、Windows Installer、Windows Phone、WMI は、Microsoft グループ企業の商標です。

Firefox、Mozilla は、米国およびその他の国における Mozilla Foundation の商標です。

Java、JavaScript は、Oracle およびその子会社の登録商標です。

Parallels、Parallels のロゴ、および Coherence は、Parallels International GmbH の商標または登録商標です。

VMware、VMware Fusion は、米国およびその他の国における VMware, Inc. の商標または登録商標です。

JAMF、Composer は、米国およびその他の国における JAMF SOFTWARE, LLC の登録商標またはコモンロー商標です。

〔パスワードで保護された圧縮ファイルを検出しました〕 ウィンドウ

ファイル脅威対策やスキャンタスク実行中に、パスワードで保護された圧縮ファイルをスキャンする必要がある場合、通知ウィンドウが表示されます。

圧縮ファイル

圧縮ファイルへのパス。

パスワード

パスワードの入力欄です。

パスワードを入力すると、Kaspersky Endpoint Security が圧縮ファイルをスキャンし、マルウェアなどのコンピュータのセキュリティの脅威の有無を確認します。

保護された圧縮ファイルをスキャンしない

このボタンをクリックすると、そのオブジェクトおよびそれと同じ種別のオブジェクトがすべてスキップされます。

スキップ

オブジェクトをスキップするには、このボタンをクリックします。

「プロキシサーバー認証が必要です」 ダイアログ

ユーザ名

プロキシサーバーへの接続に使用するユーザ名の入力欄です。

パスワード

パスワードの入力欄です。

パスワードを記憶する

指定したユーザ名とパスワードを、プロキシサーバーへの認証時に今後使用するかどうかを選択します。

既定では、このチェックボックスはオフです。

「オブジェクトを検知しました」 ダイアログ

Kaspersky Endpoint Security でウイルスなどのコンピュータセキュリティの脅威が検知された場合、通知ウィンドウが画面に表示されます。

検知

[カスペルスキーのウイルス百科事典](#) の分類に基づくオブジェクト名

詳細

このボタンをクリックすると、[カスペルスキーのウイルス百科事典](#) のページが開き、検知されたオブジェクトに関する情報を確認できます。

オブジェクト

オブジェクトの保存先フォルダのパスまたはオブジェクトが検知された Web アドレス。

選択した処理を常に実行

ファイル脅威対策、ウェブ脅威対策、マルウェアスキャンタスクの現行のセッション中に、同じ種別のすべてのオブジェクトに対して、選択した処理を有効または無効にします。

既定では、このチェックボックスはオフです。

ファイル脅威対策またはウェブ脅威対策の現行のセッションとは、コンポーネントが起動してから停止するまで、または本製品をシャットダウンまたは再起動するまでの期間を指します。マルウェアスキャンタスクの現行セッションとは、スキャンタスクの開始から完了までの期間を指します。

検知されたオブジェクトに対して実行できる処理のボタンは、検知されたオブジェクトの種別によって異なります。

次のいずれかの処理を選択できます：

- **駆除**：オブジェクトを駆除します。駆除を実行する前に、元のファイルを復元する必要がある場合に備えて、そのファイルのバックアップコピーが作成されます。
- **削除**：オブジェクトを削除します。削除を実行する前に、元のファイルを復元する必要がある場合に備えて、そのファイルのバックアップコピーが作成されます。
- **ブロックしない**：危険な Web トラフィックオブジェクトとみなされる Web サイトへのアクセスを許可します。
- **ブロック**：危険な Web トラフィックオブジェクトとみなされる Web サイトへのアクセスを拒否します。
- **圧縮ファイルを削除**：検知した脅威の入っている圧縮ファイルを削除します。
- **保護された圧縮ファイルをスキャンしない**：マルウェアスキャン中、パスワードで保護された圧縮ファイルをスキップします。
- **スキップ**：オブジェクトへのアクセスをブロックします。オブジェクトに対する処理は実行しません。

「スキャン」 ウィンドウ



このボタンをクリックすると、前のウィンドウに戻ります。



このボタンをクリックすると、次のウィンドウに進みます。



このボタンをクリックすると、「スキャン」ウィンドウに表示されているマルウェアスキャンタスクの記録をすべて削除します。

スキャンをスケジュールする

このボタンをクリックすると、完全スキャンタスクまたは簡易スキャンタスクのいずれかのスケジュールを設定するダイアログが表示されます。

🕒 簡易スキャン

このセクションの「スタート」ボタン (▶) をクリックすると、簡易スキャンタスクを実行します。

🔍 完全スキャン

このセクションの「[スタート] ボタン (🔍)」をクリックすると、完全スキャンタスクを実行します。



このボタンをクリックすると、選択したマルウェアスキャンタスクが停止します。

このボタンは、マルウェアスキャンタスクが実行中である場合にのみ表示されます。

設定

このボタンをクリックすると、「[スキャン]」タブが開き、スキャンタスクを設定できます。

選択

このボタンをクリックすると、スキャンするファイルまたはフォルダを選択するダイアログが開きます。

「[ファイルとフォルダ]」セクションの下部では、選択したファイルまたはフォルダに対して実行されたすべてのマルウェアスキャンタスクの記録を表示できます。

詳細

このボタンをクリックすると、マルウェアスキャンタスクのレポートウィンドウが表示されます。

このボタンは、スキャンタスクの上にマウスを合わせると表示されます。

スキャン履歴を消去

このボタンをクリックすると、すべてのマルウェアスキャンタスクのすべての記録が削除されます。

すべてを表示

このボタンをクリックすると、「[検知したオブジェクト]」ウィンドウが開き、検知したオブジェクトをすべて確認できます。

注意：Kaspersky Endpoint Security は、OneDrive や iCloud ストレージ、その他のクラウドストレージにあるファイルをスキャンしません。これらのファイルをスキャン範囲から除外してください。そうしないと、スキャンタスクが「感染したファイルが削除されませんでした」というエラーで終了する可能性があります。

「[検知したオブジェクト]」ウィンドウ

「[検知したオブジェクト]」セクションには、本製品が検知した悪意のあるオブジェクトが表示されます。

すべて駆除

このボタンをクリックすると、検知されたすべての悪意のあるオブジェクトに対する駆除が開始されます。

すべて無視

このボタンをクリックすると、「[検知したオブジェクト]」セクションにあるリストに表示された悪意のあるオブジェクトがすべて削除されます。

...

このボタンをクリックすると、ポップアップメニューが表示され、悪意のあるオブジェクトに対して次のいずれかの操作を選択できます：

- **駆除：**オブジェクトを駆除します。Kaspersky Endpoint Security は、悪意のあるオブジェクトを駆除する前に、そのファイルのバックアップコピーを作成します。そのため、データ消失の危険性がない状態で、ファイルを後で復元または駆除できます。
- **無視：**検知したオブジェクトのリストからオブジェクトを削除します。

「[その他のオブジェクト]」セクションには、悪意はないがコンピュータやデータに損害を与える目的でハッカーによって悪用される可能性があるオブジェクトが検知されると表示されます。

すべて削除

このボタンをクリックすると、検知したオブジェクトをコンピュータからすべて削除します。

すべて無視

このボタンをクリックすると、「[その他のオブジェクト]」セクションの検知したオブジェクトのリストから、検知したオブジェクトをすべて削除します。

...

このボタンをクリックすると、ポップアップメニューが表示され、検知したオブジェクトに対して次のいずれかの操作を選択できます：

- **削除：**検知したオブジェクトをコンピュータから削除します。
- **無視：**検知したオブジェクトのリストからオブジェクトを削除します。

「[バックアップ]」セクションには、検知したオブジェクトのバックアップコピーが表示されます。

すべて削除

このボタンをクリックすると、検知したオブジェクトのバックアップコピーがすべてコンピュータから削除されます。

...

このボタンをクリックすると、ポップアップメニューが表示され、バックアップ済みオブジェクトに対して次のいずれかの操作を選択できます：

- **バックアップコピーを削除：**検知したオブジェクトのバックアップコピーをコンピュータから削除します。
- **ファイルを復元：**リストで選択したファイルのバックアップコピーが、駆除または削除する前と同じ名前で元の位置に復元されます。元の保存場所に同じ名前のオブジェクトがある場合（たとえば、駆除前に元のファイルのコピーを作成した場合や、元のファイルを駆除した場合）、警告メッセージが表示されます。その場合は、復元されたオブジェクトの保存場所を変更するか、名前を変更します。

〔ライセンス〕 ウインドウ



このボタンをクリックすると、前のウインドウに戻ります。



このボタンをクリックすると、次のウインドウに進みます。

注意：表示されるウインドウは、アクティベーションの有無や、ライセンスまたは定額制サービスの種別に応じて異なります。

表示されている可能性がある情報は次の通りです：

- ライセンスまたは定額制サービスのステータス
- 現在のライセンス
- 予備のライセンス（ある場合）
- ライセンス種別と、現在のライセンスまたはサブスクリプションで本製品を使用できるコンピュータの数
- 現在のライセンスまたはサブスクリプションで使用可能なアプリケーションの機能
- 有効期間終了日時
- ライセンスの有効期間終了までの残りの日数

このウインドウで案内される可能性がある操作は次の通りです：

- アクティベーションコードを入力して本製品をアクティベートする。
- ライセンスの購入方法を案内する **Web** サイトへ移動する。
- 定額制サービスの更新に関する情報を案内するサービスプロバイダーの **Web** サイトを開く。
- 定額制サービスの契約状態を更新する。

Kaspersky Endpoint Security のライセンスに関する詳細情報は、組織のシステム管理者にお問い合わせください。

〔脅威対策〕 タブ

〔**全般**〕 セクションでは、マルウェアやコンピュータのセキュリティへのその他の脅威に対するコンピュータ保護を有効または無効にできます。

保護機能を有効にする

マルウェアやコンピュータのセキュリティへの脅威に対するその他のコンピュータ保護を有効または無効にします。

既定では、このチェックボックスはオンです。

セキュアな接続（HTTPS）をチェックする

暗号化された接続（HTTPS）のスキャンを有効または無効にし、危険な **Web** サイトへのユーザのアクセスをウェブコントロールがブロックした時に通知を表示するかどうかを選択します。

既定では、このチェックボックスはオフです。

信頼ゾーン

このボタンをクリックすると、マルウェアをスキャンしない信頼済みオブジェクトのリストを作成して、信頼ゾーンを編集するウインドウが開きます。

設定

このボタンをクリックすると、信頼されたルート証明書の一覧を管理し、**Mozilla Firefox** ブラウザで暗号化された HTTPS トラフィックをチェックするための証明書ストアを選択できるウインドウが開きます。

〔**ファイル脅威対策**〕 セクションでは、ファイル脅威対策を有効または無効にし、感染したファイルが検知された場合に実行する処理を選択できます。

ファイル脅威対策を有効にする

ファイル脅威対策を有効または無効にします。

既定では、このチェックボックスはオンです。

保護範囲

このボタンをクリックすると表示されるウインドウで、保護範囲を作成できます。

悪意のあるオブジェクトを自動的に駆除または削除する

感染したファイルへのアクセスはブロックされ、ファイルが自動的に駆除されます。駆除を実行する前に、ファイルのバックアップコピーがバックアップに保存されます。ファイルが駆除されると、元の保存場所に元のファイル名で保存されます。駆除に失敗した場合、感染したファイルはブロックした状態で元の保存場所に置かれます。この感染したオブジェクトの検知に関する情報は、[処理されたオブジェクト](#)のレポートに記録されます。

手動選択

ファイルに感染した可能性がある悪意のあるオブジェクトの情報が通知ウィンドウに表示され、実行する処理を選択するよう要求されます。処理は、オブジェクトのステータスによって異なる場合があります。

既定では、この処理が選択されています。

「**ウェブ脅威対策**」セクションでは、ウェブ脅威対策を有効または無効にし、危険な **Web** トラフィックオブジェクトを検知した場合に実行する処理を選択できます。

ウェブ脅威対策を有効にする

ウェブ脅威対策を有効または無効にします。

既定では、このチェックボックスはオンです。

危険な Web トラフィックオブジェクトを自動的にブロックする

Kaspersky Endpoint Security は、確認を要求せずに危険な **Web** トラフィックオブジェクトが検知された **Web** サイトへのアクセスをブロックします。

手動選択

検知された危険な **Web** トラフィックオブジェクトに関する情報が通知ウィンドウに表示され、実行する処理を選択するよう要求されます。処理は、オブジェクトのステータスによって異なる場合があります。

既定では、この処理が選択されています。

「**メール脅威対策**」セクションでは、メール脅威対策を有効にするかどうかを選択し、悪意のあるオブジェクトを検知した場合に実行する処理を選択できます。

メール脅威対策を有効にする

メール脅威対策を有効または無効にします。

既定では、このチェックボックスはオンです。

悪意のあるオブジェクトを自動で削除する

Kaspersky Endpoint Security は、メール内に感染したオブジェクトを検出すると、感染したオブジェクトを削除し、オブジェクトの内容を「The requested file infected with <ウイルス名> has been deleted」というテキストに置き換えます。

悪意のあるオブジェクトを自動でブロックする

Kaspersky Endpoint Security は、メール内に感染したオブジェクトを検出すると、メールの件名を「Message is infected: <元の件名>」、という形式に置き換えます。メールの件名は、POP3 プロトコルの場合にのみ置き換えられます。

「**ネットワーク脅威対策**」セクションでは、ネットワーク攻撃からの保護を有効または無効にできます。

ネットワーク脅威対策を有効にする

ネットワーク脅威対策を有効または無効にします。

既定では、このチェックボックスはオンです。

設定

このボタンをクリックすると、信頼するコンピュータのリストを作成したり、ブロック対象のコンピュータのリストを表示および編集できるウィンドウが表示されます。



このボタンをクリックすると、管理者権限を持たないユーザによる Kaspersky Endpoint Security の設定の変更を防止できます。



このボタンをクリックすると、管理者の認証情報を入力する画面が表示されます。管理者の認証情報を入力すると、本製品の設定が編集可能になります。

「保護範囲」 ウィンドウ

「**保護範囲**」セクションでは、保護範囲の確認と編集が行えます。

すべてのリムーバブルディスク

すべてのリムーバブルディスクのリアルタイム保護を有効または無効にします。

既定では、このチェックボックスはオンです。

すべての内部ディスク

すべての内部ディスクのリアルタイム保護を有効または無効にします。

既定では、このチェックボックスはオンです。

すべてのネットワークディスク

すべてのネットワークドライブのリアルタイム保護を有効または無効にします。

既定では、このチェックボックスはオンです。

+

このボタンをクリックすると、保護範囲を作成するための項目を選択できるリストが表示されます：

- **ファイルとフォルダ**：この項目を選択すると、保護範囲にファイルまたはフォルダを追加するためのダイアログが表示されます。
- **すべてのディスク**：この項目を選択すると、コンピュータのすべてのリムーバブルディスク、内部ディスク、ネットワークドライブが保護範囲に追加されます。
- **すべてのリムーバブルディスク**：この項目を選択すると、コンピュータのすべてのリムーバブルディスクが保護範囲に追加されます。
- **すべての内部ディスク**：この項目を選択すると、コンピュータのすべての内部ディスクが保護範囲に追加されます。
- **すべてのネットワークディスク**：この項目を選択すると、コンピュータのすべてのネットワークドライブが保護範囲に追加されます。
- **メモリ**：この項目を選択すると、コンピュータのメモリが保護範囲に追加されます。
- **スタートアップオブジェクト**：この項目を選択すると、オペレーティングシステムの起動時に起動されるすべての実行ファイルが保護範囲に追加されます。スタートアップオブジェクトをスキャンするとルートキットを検知できます。

リスト項目の横のチェックボックスで、その項目に関連するオブジェクトのリアルタイム保護を有効または無効にします。

–

このボタンをクリックすると、保護範囲リストから選択した項目が削除されます。

保護範囲リストに既定で含まれる項目は削除できません。

〔最適化〕セクションで、スキャンタスクの実行時に読み取り専用のシステムボリュームをスキャンするかどうかを設定できます。

読み取り専用のシステムボリュームのスキャンをスキップする

読み取り専用のシステムボリュームのスキャンをスキップするかどうかを選択します。

既定では、このチェックボックスはオンです。

重要：最適化の操作が、セキュリティ上の理由から無効化される場合があります。

〔設定〕 ウィンドウ

〔信頼済みコンピュータ〕タブでは、信頼するコンピュータのリストを作成できます。**Kaspersky Endpoint Security** は、このリストに含まれるコンピュータからの危険なネットワーク活動を検知した場合でも、それらの IP アドレスを自動的にブロックしません。

既定では、信頼するコンピュータのリストは空白になっています。

+

このボタンをクリックすると、信頼するコンピュータの IP アドレスの入力欄が追加されます。

–

このボタンをクリックすると、選択した IP アドレスが信頼するコンピュータのリストから削除されます。

編集

このボタンをクリックすると、選択した IP アドレスを編集できるようになります。

〔ブロック対象コンピュータ〕タブでは、ブロック対象のコンピュータのリストを表示して、編集できます。

この IP アドレスを持つコンピュータで危険なネットワーク活動が検知された場合、検知から 1 時間、このコンピュータがブロックされます。

IP アドレス

この列には、ブロック対象のコンピュータの IP アドレスが表示されます。

発生時刻

この列には、コンピュータで危険なネットワーク活動が検知された日時が表示されます。

ブロック解除

このボタンをクリックすると、選択した IP アドレスがブロック対象のコンピュータのリストから削除されます。

〔スキャン〕 タブ

マルウェアスキャンタスクのリスト

設定されているマルウェアスキャンの種別は次の通りです：

-  **完全スキャン**：コンピュータのメモリ、スタートアップオブジェクト、コンピュータのすべての内部ディスクをスキャンします。
-  **簡易スキャン**：コンピュータの重要領域（メモリ、スタートアップオブジェクト、システムフォルダ）のみをスキャンします。
-  **オブジェクトスキャン**：指定されたオブジェクト（ファイル、フォルダ、内部ディスク、リムーバブルディスク）をスキャンします。

-  **外部ディスクのスキャン**：外部ディスクがコンピュータに接続された時に、外部ディスクに対してマルウェアスキャンを実行します。

注意：Kaspersky Endpoint Security は、OneDrive や iCloud ストレージ、その他のクラウドストレージにあるファイルをスキャンしません。これらのファイルをスキャン範囲から除外してください。そうしないと、スキャンタスクが「感染したファイルが削除されませんでした」というエラーで終了する可能性があります。

〔**スキャン範囲**〕 セクションでは、簡易スキャンタスクのスキャン範囲を表示し、編集することができます。

編集

このボタンをクリックすると、スキャン範囲が表示され、編集することができます。

簡易スキャンタスクがリストで選択されている場合にのみ、このボタンが表示されます。

〔**処理**〕 セクションでは、感染したファイルの検知時に Kaspersky Endpoint Security が実行する処理を選択し、タスクをスケジュールできます。

悪意のあるオブジェクトを自動的に駆除または削除する

感染したファイルへのアクセスはブロックされ、ファイルが自動的に駆除されます。駆除を実行する前に、ファイルのバックアップコピーがバックアップに保存されます。ファイルが駆除されると、元の保存場所に元のファイル名で保存されます。駆除に失敗した場合、感染したファイルはブロックした状態で元の保存場所に置かれます。この感染したオブジェクトの検知に関する情報は、[処理されたオブジェクト](#) のレポートに記録されます。

スキャン完了時に手動選択

感染したファイルに対する処理が、検知してからスキャンが完了するまで延期されます。スキャンが完了すると、検知された感染したオブジェクトに関する情報が通知が表示され、実行する処理を選択できます。処理は、オブジェクトのステータスによって異なる場合があります。

既定では、この処理が選択されています。

〔**外部ディスクのスキャン**〕 タブの 〔**外部ディスクの接続時**〕 セクションで、外部ディスクの接続時に実行される処理を選択できます。

スキャン

このオプションをオンにすると、Kaspersky Endpoint Security は接続された外部ディスクのマルウェアスキャンタスクを開始します。

既定では、このオプションがオンです。

何もしない

このオプションをオンにすると、Kaspersky Endpoint Security は接続された外部ディスクをスキャンしません。

〔**最適化**〕 セクションで、簡易スキャンまたは完全スキャンの実行時に読み取り専用のシステムボリュームをスキャンするかどうかを設定できます。

読み取り専用のシステムボリュームのスキャンをスキップする

読み取り専用のシステムボリュームのスキャンをスキップするかどうかを選択します。

既定では、このチェックボックスは簡易スキャンタスクでオンで、完全スキャンタスクではオフです。

重要：最適化の操作が、セキュリティ上の理由から無効化される場合があります。

CPU 使用率

このボタンをクリックすると、スキャンタスク用に保護対象デバイスの CPU の使用を有効または無効にするダイアログが表示されます。〔**スキャンによる CPU 使用率を制限する**〕 をオンにすると、許可する CPU 使用率の上限に対応するフィールドに指定できます。

注意：この制限は、すべての CPU コアからの累積に対して適用されます。アクティビティモニタに表示される CPU 使用率は、各 CPU コアの使用率の合計であり、そのため、100 % を超えた数値が表示される場合があります。

このオプションをオンにすると、Kaspersky Endpoint Security のパフォーマンスが低下する可能性があります。

既定では、このオプションはオフです。

スケジュール

このボタンをクリックすると、完全スキャンタスクまたは簡易スキャンタスクのいずれかのスケジュールを設定するダイアログが表示されます。



このボタンをクリックすると、管理者権限を持たないユーザによる Kaspersky Endpoint Security の設定の変更を防止できます。



このボタンをクリックすると、管理者の認証情報を入力する画面が表示されます。管理者の認証情報を入力すると、本製品の設定が編集可能になります。

「スキャン範囲」 ウインドウ

このボタンをクリックすると、簡易スキャンの範囲が表示され、編集することができます。

オブジェクトの隣のチェックボックスで、そのオブジェクトをスキャンするかどうかを選択できます。

+

このボタンをクリックすると、スキャン範囲を調整するリストが表示されます：

- **ファイルとフォルダ**：この項目を選択すると、スキャン範囲にファイルまたはフォルダを追加するためのダイアログが表示されます。
- **すべてのディスク**：この項目を選択すると、コンピュータのすべてのリムーバブルドライブ、内部ドライブ、ネットワークドライブがスキャン範囲に追加されます。
- **「すべての外部ディスク」**：この項目を選択すると、コンピュータのすべてのリムーバブルディスクがスキャン範囲に追加されます。
- **すべての内部ディスク**：この項目を選択すると、コンピュータのすべての内部ディスクがスキャン範囲に追加されます。
- **すべてのネットワークディスク**：この項目を選択すると、コンピュータのすべてのネットワークドライブがスキャン範囲に追加されます。
- **メモリ**：この項目を選択すると、コンピュータのメモリがスキャン範囲に追加されます。
- **スタートアップオブジェクト**：この項目を選択すると、オペレーティングシステムの起動時に起動されるすべての実行ファイルがスキャン範囲に追加されます。スタートアップオブジェクトをスキャンするとルートキットを検知できます。

–

このボタンをクリックすると、スキャン範囲リストから選択した項目が削除されます。

スキャン範囲リストに既定で含まれる項目は削除できません。

「最適化」セクションで、スキャンタスクの実行時に読み取り専用のシステムボリュームをスキャンするかどうかを設定できます。

読み取り専用のシステムボリュームのスキャンをスキップする

読み取り専用のシステムボリュームのスキャンをスキャンするかどうかを選択します。

このチェックボックスをオンにすると、読み取り専用のシステムボリュームのスキャンがスキップされ、スキャンにかかる時間が大幅に短縮されます。

このチェックボックスをオフにすると、読み取り専用のシステムボリュームをスキャンします。

既定では、このチェックボックスはオンです。

注意：Kaspersky Endpoint Security は、OneDrive や iCloud ストレージ、その他のクラウドストレージにあるファイルをスキャンしません。これらのファイルをスキャン範囲から除外してください。そうしないと、スキャンタスクが「感染したファイルが削除されませんでした」というエラーで終了する可能性があります。

「脅威」 タブ

「検知するオブジェクト」セクションで、検知対象のオブジェクトのリストを設定できます。

ウイルス、ワーム、トロイの木馬、悪意のあるツール、アドウェア、オートダイアラー

カテゴリに含まれるプログラム種別は次の通りです：

- すべての種別のマルウェア。
- コンピュータで広告（バナーなど）を表示したり、Web ブラウザでの検索結果を Web サイトの広告に置き換えたりするアプリケーション。
- 利用者の許可なくコンピュータのモデムによる電話回線接続を確立するアプリケーション。

Kaspersky Endpoint Security では、この種別のプログラムを常に制御します。

このチェックボックスは必ずオンになっています。オフにすることはできません。

ユーザに損害を与える目的で悪用される可能性がある正規のソフトウェア

ユーザに損害を与える目的で悪用される可能性がある合法ソフトウェア（リモート管理アプリケーションなど）の制御を有効または無効にします。

既定では、このチェックボックスはオフです。

「バックアップ」セクションでは、バックアップにオブジェクトを保存する最長期間を指定できます。

バックアップを削除するまでの期間：<数字> 日

指定した期間の経過後、バックアップからのオブジェクトを削除するかどうかを選択します。

このチェックボックスをオンにすると、チェックボックスに隣接する入力フィールドで指定した期間の経過後、バックアップからオブジェクトが削除されます。オフにすると、バックアップ内のオブジェクトは無期限に保存されます。

既定では、このチェックボックスはオンで、オブジェクトはバックアップに 30 日間保存されます。

〔除外〕セクションで、信頼できると判断してマルウェアスキャンの対象にしないファイル、フォルダ、アプリケーション、Web サイトのリストを作成できます。

信頼ゾーン

このボタンをクリックすると、除外リストを編集するためのウインドウが表示されます。

注意：管理者が信頼ゾーンの編集を禁止するようにポリシーを設定すると、ユーザは信頼ゾーンの設定に移動できなくなります。



このボタンをクリックすると、管理者権限を持たないユーザによる Kaspersky Endpoint Security の設定の変更を防止できます。



このボタンをクリックすると、管理者の認証情報を入力する画面が表示されます。管理者の認証情報を入力すると、本製品の設定が編集可能になります。

管理者パスワードのセットアップウインドウ

パスワード

ユーザのデバイス上での不要な操作を制限するためのパスワードを入力するフィールド。

パスワードの確認

パスワードを再度入力して確認するためのフィールド。

オプション

パスワードで保護できる操作のリスト。ユーザのデバイス上の対応する操作を保護するには、必要なチェックボックスをオンにします。少なくとも 1 つのチェックボックスを選択する必要があります。

キャンセル

このボタンをクリックすると、変更を保存せずにウインドウを閉じます。

OK

このボタンをクリックすると、管理者パスワード設定が保存され、ウインドウが閉じます。変更を保存すると、デバイス上で不要な操作を実行しようとするパスワードの入力が要求されるようになります。

〔パスワードによる保護の設定〕 ウインドウ

パスワード

ユーザのデバイス上での不要な操作を制限するためのパスワードを入力するフィールド。
入力した記号を表示するには、〔表示〕をクリックします。

パスワードの確認

パスワードを再度入力して確認するためのフィールド。
入力した記号を表示するには、〔表示〕をクリックします。

パスワードが必要な操作

パスワードで保護できる操作のリスト。ユーザのデバイス上の対応する操作を保護するには、必要なチェックボックスをオンにします。

〔信頼済みアプリケーション〕 タブ

〔信頼済みアプリケーション〕タブで、Kaspersky Endpoint Security で監視する必要のないアプリケーションのリストを作成できます。

既定では、信頼ゾーンのオブジェクトのリストは空白になっています。



このボタンをクリックすると、[アプリケーションのパスを入力したり、監視しない種別の活動を選択するウインドウ](#)が表示されます。

—

このボタンをクリックすると、選択したアプリケーションが信頼ゾーンから削除されます。

編集

このボタンをクリックすると、信頼済みアプリケーションのパラメータを編集するためのウインドウが表示されます。

[信頼済みアプリケーションの追加] ウインドウ

パス

活動が監視されないアプリケーションへのパス。

注意：このフィールドでのパスの指定にシンボリックリンクを使用することはできません。

選択

このボタンをクリックするとウインドウが開き、ネットワーク活動が監視されないアプリケーションへのパスを入力できます。この場合、[パス] および [コード署名の要件] フィールドの値が自動的に挿入されます。

コード署名の要件

Kaspersky Endpoint Security によって活動が監視されないアプリケーションのコード署名の要件。

これはオプションのパラメータです。

[オプション] セクションでは、監視しない活動の種別を選択できます。

ファイル操作を監視しない

クライアントコンピュータ上のファイルを使用したアプリケーションの動作の監視を有効または無効にします。

このチェックボックスをオンにすると、アプリケーションのファイルの動作は監視されません。

このチェックボックスをオフにすると、アプリケーションのファイルの動作を監視します。

既定では、このチェックボックスはオンです。

ネットワーク活動を監視しない

クライアントコンピュータ上のアプリケーションが送受信するインターネットトラフィックの監視を有効または無効にします。

このチェックボックスをオンにすると、アプリケーションのネットワーク活動は監視されません。

このチェックボックスをオフにすると、アプリケーションのネットワーク活動を監視します。

既定では、このチェックボックスはオンです。

キャンセル

このボタンをクリックすると、変更を保存せずにウインドウを閉じます。

OK

このボタンをクリックすると、信頼済みアプリケーションのパラメータが保存され、ウインドウが閉じます。

[信頼するファイルとフォルダ] タブ

[ファイルとフォルダ] タブで、Kaspersky Endpoint Security で監視する必要のないファイルとフォルダのリストを作成できます。

既定では、信頼ゾーンは空白になっています。

+

このボタンをクリックすると、ファイルまたはフォルダを開くダイアログが表示されます。

—

このボタンをクリックすると、選択したオブジェクトが信頼ゾーンから削除されます。

[信頼する URL] タブ

[URL] タブで、Kaspersky Endpoint Security で監視する必要のない URL のリストを作成できます。

既定では、信頼ゾーンは空白になっています。

+

このボタンをクリックすると、URL を入力するフィールドが追加されます。

Web サイトのアドレスを指定するときに、次の記号を使用できます：

- アスタリスク（*）は、\ と / を除くすべての文字の代わりとして使用できます。
- 連続する 2 つのアスタリスク（**）は、\ と / を含む 文字任意の文字列（空の文字列を含む）の代わりに使用できます。
- 疑問符（?）は、ファイル名またはフォルダ名の任意の 1 文字（\ と / を除く）の代わりになります。

–

このボタンをクリックすると、選択した URL が信頼ゾーンから削除されます。

〔詳細〕 タブ

〔KSN〕セクションで、Kaspersky Security Network に関する声明を確認し、Kaspersky Security Network に参加するかどうかを選択できます。

KSN 声明を表示する

このボタンをクリックすると、Kaspersky Security Network の声明の全文が表示されます。

KSN のインフラストラクチャは、グローバルまたはプライベートを使用できます。Kaspersky Security Network に参加する場合、本製品はファイル、Web リソース、アプリケーションの評価に関する情報を Kaspersky Security Network から受信して使用し、検知サービスに必要なデータを Kaspersky Security Network に提供します。

Kaspersky Security Network に参加する

Kaspersky Security Network への参加を有効または無効にします。

Kaspersky Private Security Network に参加する

Kaspersky Private Security Network への参加を有効または無効にします。Kaspersky Private Security Network への参加に関する詳細情報は、組織のシステム管理者にお問い合わせください。

拡張 KSN モードを有効にする

コンピュータの保護機能と本製品のユーザビリティの向上に必要な詳細データを、カスペルスキーに提供するかどうかなを選択します。Kaspersky Security Network に関する声明と Kaspersky Endpoint Security のヘルプで、提供するデータのリストを確認できます。

このチェックボックスは、〔Kaspersky Security Network に参加する〕をオンにすると自動的にオンになりますが、オフにすることもできます。

クラウドモードを有効にする

クラウドモードは、Kaspersky Endpoint Security でライト版の定義データベースを使用する動作モードです。このモードは、Kaspersky Security Network への参加が有効な場合にのみ使用可能です。ライト版の定義データベースを使用すると、コンピュータのメモリの使用量を、これ以外の場合の通常の定義データベースで 사용되는量の約半分にすることができます。Kaspersky Security Network に参加していない、またはクラウドモードが無効になっている場合は、カスペルスキーのサーバから完全版の定義データベースがダウンロードされます。

スイッチをオンにすると、ライト版の定義データベースが使用され、オペレーティングシステムリソースの負荷が軽減されます。

注意：ライト版の定義データベースは、チェックボックスをオンにした後の次のアップデート中にダウンロードされます。

スイッチをオフにすると、完全版の定義データベースが使用されます。

注意：完全版の定義データベースは、チェックボックスをオフにした後の次のアップデート中にダウンロードされます。

ふるまい検知セクションでは、ふるまい検知コンポーネントを有効または無効にし、マルウェア活動の検知時に実行するアクションを選択できます。

ふるまい検知を有効にする

このチェックボックスは、コンピュータ上のアプリケーションの動作に関する情報を受信し、それを他の保護コンポーネントに提供してパフォーマンスを向上させるふるまいコンポーネントを有効または無効にします。

マルウェアの動作をブロックする

このオプションをオンにすると、Kaspersky Endpoint Security は悪意のある活動の検知時にアプリケーションを終了します。

検知した危険なオブジェクトを削除する

このオプションをオンにすると、悪意のある活動の検知時に Kaspersky Endpoint Security は悪意のあるアプリケーションの実行ファイルを削除し、バックアップにファイルのバックアップコピーを作成します。

手動選択

このオプションをオンにすると、マルウェア活動の検知時に、悪意のあるオブジェクトに関する情報が通知ウィンドウに表示されて、Kaspersky Endpoint Security が実行する処理を選択するようユーザーに要求します。実行可能な処理は、オブジェクトの状態によって異なる場合があります。



このボタンをクリックすると、管理者権限を持たないユーザによる Kaspersky Endpoint Security の設定の変更を防止できます。



このボタンをクリックすると、管理者の認証情報を入力する画面が表示されます。管理者の認証情報を入力すると、本製品の設定が編集可能になります。

〔アップデート〕 タブ

〔定義データベース〕 セクションで、定義データベースのアップデートのモードを設定できます。

自動的にアップデートをダウンロードする

定義データベースを自動的にアップデートするかどうかを選択します。

既定では、このチェックボックスはオンです。

〔プロキシ〕 セクションでは、Kaspersky Endpoint Security のアップデートで使用するプロキシサーバを設定できます。

プロキシサーバを使用する

定義データベースとソフトウェアモジュールのアップデート時にプロキシサーバを使用してインターネットに接続するかどうかを選択します。

既定では、このチェックボックスはオンです。

設定

このボタンをクリックすると、プロキシサーバ接続の設定を編集できるウィンドウが表示されます。

〔ロールバック〕 セクションでは、定義データベースを以前のバージョンにロールバックできます。定義データベースの新しいバージョンに正しくないシグネチャが含まれていて、安全なアプリケーションをブロックしてしまう場合、アップデートのロールバックが必要になることがあります。

アップデートのロールバック

このボタンをクリックすると、定義データベースのロールバックが実行されます。



このボタンをクリックすると、管理者権限を持たないユーザによる Kaspersky Endpoint Security の設定の変更を防止できます。



このボタンをクリックすると、管理者の認証情報を入力する画面が表示されます。管理者の認証情報を入力すると、本製品の設定が編集可能になります。

〔プロキシサーバ設定〕 ウィンドウ

システムのプロキシサーバ設定を使用する

Mac のシステム設定で指定されたプロキシサーバ設定を使用します。

既定では、この処理が選択されています。

指定したプロキシサーバ設定を使用する

このウィンドウで指定されたプロキシサーバ設定を使用します。

アドレス

プロキシサーバの IP アドレスまたはドメイン名の入力欄です。

このフィールドは、〔指定したプロキシサーバ設定を使用する〕 をオンにすると使用できます。

ポート

Kaspersky Endpoint Security のアップデートに使用するプロキシサーバのポート番号の入力欄です。

このフィールドは、〔指定したプロキシサーバ設定を使用する〕 をオンにすると使用できます。

既定では 8080 です。

認証を使用する

認証とは、プロキシサーバへの接続時にユーザ名とパスワードを検証するプロセスです。

プロキシサーバへの接続時の認証を有効または無効にします。

既定では、このチェックボックスはオフです。

ユーザ名

プロキシサーバへの接続時に認証するユーザ名の入力欄です。

このフィールドは、〔認証を使用する〕 をオンにすると使用できます。

パスワード

プロキシサーバへの接続時に認証するパスワードの入力欄です。

このフィールドは、〔認証を使用する〕 をオンにすると使用できます。

ユーザ名とパスワードを指定していない場合や、指定したユーザ名とパスワードがプロキシサーバに拒否された場合は、プロキシサーバでの認証のためのユーザ名とパスワードを入力するウインドウが表示されます。認証が正常に行われ、入力ウインドウの「**パスワードを記憶する**」がオンになっている場合、指定したユーザ名とパスワードは、その後、常に使用されます。ユーザ名とパスワードを入力するウインドウの「**パスワードを記憶する**」がオフになっていると、プロキシサーバへの次回接続時にユーザ名とパスワードを再度入力する必要があります。

ローカルアドレスにはプロキシサーバを使用しない

このチェックボックスでは、ローカルフォルダまたはネットワークフォルダからアップデートを行う際に、プロキシサーバを使用するかどうかを選択します。

既定では、このチェックボックスはオンです。

「インターフェイス」タブ

「**通知**」セクションで、様々なイベントの発生時に本製品が表示する通知を設定できます。

通知を有効にする

製品のイベントに関する通知を有効または無効にします。

既定では、このチェックボックスはオンです。

マルウェアの検知時に警告音を鳴らす

悪意のあるオブジェクトの検知時に音を鳴らすかどうかを選択します。

既定では、このチェックボックスはオンです。

「**製品アイコン**」セクションでは、メニューバーでの製品アイコンの表示を設定できます。

メニューバーに表示する

メニューバーに製品アイコンを表示するかどうかを選択します。

「**レポート**」セクションでは、重要なイベント以外にも Kaspersky Endpoint Security のレポートに記録するかどうかを選択できます。

緊急イベント以外も記録する

情報イベントをレポートに保存するかどうかを選択します。通常、このようなイベントはコンピュータを保護する上で重要ではありません。

「**トレース**」セクションで、トレースを有効または無効にできます。

トレースは、アプリケーションの活動の詳細情報を記録する効果的な手段です。カスペルスキーのテクニカルサポートでは、問題の解決にトレースファイルを使用します。アプリケーションのイベント記録を有効にし、トレースファイルを作成して、テクニカルサポートが要求する場合にそれらを提供できます。既定では、アプリケーションのログ記録は無効にされています。

重要：トレースは、テクニカルサポートの担当者から指示された場合にのみ有効にしてください。

トレースを有効にする

トレースファイルを作成するかどうかを選択します。

既定では、このチェックボックスはオフです。

「**パスワードによる保護**」セクションでは、コンピュータ上の不要な操作に対するパスワードによる保護を有効にすることができます。

パスワードによる保護を有効にする

このチェックボックスは、不要な操作のパスワードによる保護を有効または無効に設定します。

既定では、このチェックボックスはオフです。

このチェックボックスをオンにすると、[管理者パスワードを設定および編集するウインドウ](#)が開きます。

設定

このボタンをクリックすると、[管理者パスワードのパラメータを編集するウインドウ](#)が表示されます。



このボタンをクリックすると、管理者権限を持たないユーザによる Kaspersky Endpoint Security の設定の変更を防止できます。



このボタンをクリックすると、管理者の認証情報を入力する画面が表示されます。管理者の認証情報を入力すると、本製品の設定が編集可能になります。

「メール脅威対策の設定」ウインドウ

次のサイズ以上のアーカイブをスキップする：NMB

このチェックボックスをオンにすると、メールメッセージに添付されたアーカイブのサイズが指定値を超える場合に、メール脅威対策によって、そのアーカイブがスキャンから除外されます。

このチェックボックスをオフにすると、メール脅威対策によって、あらゆるサイズのメール添付のアーカイブがスキャンされます。

既定値は 8 MB です。

既定では、このチェックボックスはオンです。

アーカイブのスキャンの時間を制限する

このチェックボックスをオンにすると、メールメッセージに添付されたアーカイブのスキャンに割り当てられる時間が、指定された期間に制限されます。

このチェックボックスをオフにすると、アーカイブのスキャンに割り当てられる時間は制限されません。

既定値は **5 秒** です。

既定では、このチェックボックスはオンです。

「ネットワークパケットルール」 ウィンドウ

ルール名

ネットワークパケットルールの名前。

「**処理**」 セクションで、ネットワーク活動の検知時に **Kaspersky Endpoint Security** によって実行される処理を選択できます。

「**プロトコル**」 セクションで、ネットワークルールが適用されるプロトコルを指定できます。

「**方向**」 セクションで、監視対象のネットワーク活動の方向を指定できます。

「**TTL**」 セクションで、監視対象のネットワークパケットの有効期間を指定できます。

「**ネットワークアダプター**」 セクションで、ネットワークルールが適用されるネットワークアダプターを指定できます。

「**リモートアドレス**」 セクションで、ネットワークパケットを送受信できるリモートデバイスのネットワークアドレスを指定できます。

「**ローカルアドレス**」 セクションで、ネットワークパケットを送受信できるデバイスのローカルネットワークアドレスを指定できます。

イベントを記録

ファイアウォールのイベントをレポートに保存するかどうかを選択します。

このチェックボックスをオンにすると、ファイアウォールのイベントがレポートに記録されます。

このチェックボックスをオフにすると、ファイアウォールのイベントはレポートに記録されません。

既定では、このチェックボックスはオフです。

「ネットワークアダプター」 ウィンドウ

アダプター名

ネットワークアダプターの名前。

インターフェイス種別

このドロップダウンリストから、ネットワークアダプターのインターフェイス種別を選択できます。

IP アドレス

IP アドレスのリスト。

MAC アドレス

MAC アドレスのリスト。

「ネットワークアダプター」 ウィンドウ

名前

この列には、ネットワークアダプターの名前が表示されます。

インターフェイス種別

この列には、ネットワークアダプターのインターフェイス種別が表示されます。

IP アドレス

この列には、ネットワークアダプターの **IP アドレス** が表示されます。

MAC アドレス

この列には、ネットワークアダプターのコンピュータの **MAC アドレス** が表示されます。

「ローカルアドレス」 ウィンドウ

ローカルアドレス

この列には、ローカルアドレスが表示されます。

「ローカルアドレス」 ウィンドウ

種別

このドロップダウンリストでは、ネットワークルールを適用するローカル **IP** のエントリの種別を指定できます。

IP アドレス

IP アドレスの入力フィールド。このフィールドは、「**種別**」 ドロップダウンリストで 「**IP アドレス**」 を選択した場合にのみ使用可能です。

範囲の開始

IP アドレスの範囲の開始の入力フィールド。このフィールドは、**[種別]** ドロップダウンリストで **[IP アドレスの範囲]** を選択した場合にのみ使用可能です。

範囲の終了

IP アドレスの範囲の終了の入力フィールド。このフィールドは、**[種別]** ドロップダウンリストで **[IP アドレスの範囲]** を選択した場合にのみ使用可能です。

[リモートアドレス] ウインドウ

リモートアドレス

この列には、リモートアドレスが表示されます。

[リモートアドレス] ウインドウ

種別

このドロップダウンリストでは、ネットワークルールを適用するリモートアドレスのエントリの種別を指定できます。

アドレス

IP アドレスまたは DNS 名の入力フィールド。このフィールドは、**[種別]** ドロップダウンリストで **[IP アドレスまたは DNS 名]** を選択した場合にのみ使用可能です。

範囲の開始

IP アドレスの範囲の開始の入力フィールド。このフィールドは、**[種別]** ドロップダウンリストで **[IP アドレスの範囲]** を選択した場合にのみ使用可能です。

範囲の終了

IP アドレスの範囲の終了の入力フィールド。このフィールドは、**[種別]** ドロップダウンリストで **[IP アドレスの範囲]** を選択した場合にのみ使用可能です。

[テンプレート] ウインドウ

ネットワークルールテンプレート

この列には、ネットワークルールテンプレートが表示されます。

[ネットワークパケットルール] タブ

ネットワークサービス

ネットワークルールの名前

処理

ネットワーク動作の種類の検知時にファイアウォールが実行する処理

アドレス

ネットワークルールが適用されるネットワークアドレス。

[使用可能なネットワーク] タブ

名前

この列には、ネットワーク名が表示されます。

ネットワークのステータス

この列には、ネットワークのステータスが表示されます。

IP アドレス

この列には、ネットワークの IP アドレスが表示されます。

[使用可能なネットワーク] ウインドウ

ネットワーク名

ネットワークの名前

ネットワークのステータス

ネットワークのステータスのドロップダウンリスト。

IP アドレス

ネットワークの IP アドレス。

[MAC アドレス] ウィンドウ

種別

このドロップダウンリストでは、ネットワークルールを適用する MAC アドレスのエントリの種別を指定できます。

MAC アドレス

MAC アドレスの入力フィールド。このフィールドは、**[種別]** ドロップダウンリストで **[MAC アドレス]** を選択した場合にのみ使用可能です。

マスク

MAC アドレスマスクの入力フィールド。このフィールドは、[種別] ドロップダウンリストで [MAC アドレスマスク] を選択した場合にのみ使用可能です。

範囲の開始

MAC アドレスの範囲の開始の入力フィールド。このフィールドは、[種別] ドロップダウンリストで [MAC アドレスの範囲] を選択した場合にのみ使用可能です。

範囲の終了

MAC アドレスの範囲の終了の入力フィールド。このフィールドは、[種別] ドロップダウンリストで [MAC アドレスの範囲] を選択した場合にのみ使用可能です。

システムイベントレポート

ウィンドウ右側のペインに、本製品の動作に関するレポートが表示されます。

時間

この列には、イベントの日時が表示されます。

イベント

この列には、イベントのステータスが表示されます。

プログラム名

この列には、イベントが発生したプログラムの名前が表示されます。

ユーザ

この列には、このイベントを開始したユーザの名前が表示されます。

ユーザ種別

この列には、このイベントを開始したユーザの種別が表示されます。



このボタンをクリックすると、レポートをTXTファイルで保存するためのウィンドウが表示されます。

処理されたオブジェクトのレポート

ウィンドウの右側に、Kaspersky Endpoint Security が検知したすべての感染したオブジェクトおよび危険な Web トラフィックオブジェクトのリストが表示されます。

時間

この列には、オブジェクトが検知された時間が表示されます。

オブジェクト

この列には、オブジェクトが検知された場所へのパスか、オブジェクトの URL が表示されます。

ステータス

この列には、オブジェクトの検知後に本製品が実行した処理が表示されます。

検知

この列には、カスペルスキーのウイルス百科事典の分類に従って、検知した脅威の種別が表示されます。

名前

この列には、カスペルスキーのウイルス百科事典の分類に従って、検知した脅威の名前が表示されます。



このボタンをクリックすると、レポートをTXTファイルで保存するためのウィンドウが表示されます。

定義データベースのアップデートのレポート

ウィンドウの右ペインに、本製品が実行したアップデートタスクのレポートが表示されます。

開始

この列には、各アップデートタスクの開始日時が表示されます。処理のリストを展開すると、この列には、本製品のアップデート中に実行された処理と、それらの処理が実行された時間もリストされます。

ステータス

この列には、アップデートタスクのステータスが表示されます。

サイズ

この列には、ダウンロードしたアップデートファイルのサイズが表示されます。

平均速度

この列には、アップデートファイルのダウンロード速度が表示されます。

終了

この列には、アップデートの終了日時が表示されます。



このボタンをクリックすると、アップデートに含まれる操作のリストが展開されます。



このボタンをクリックすると、アップデートに含まれる操作のリストが縮小されます。



このボタンをクリックすると、レポートをTXTファイルで保存するためのウインドウが表示されます。

スキヤンのレポート

ウインドウの右ペインに、本製品が実行したスキヤンタスクのレポートが表示されます。

タスク

この列には、スキヤンタスクの名前が表示されます。

ステータス

この列には、スキヤンタスクのステータスカ、スキヤン済みオブジェクトのステータスが表示されます。

日付

この列には、スキヤンタスクの日時が表示されます。

イニシエータ

この列には、スキヤンタスクを開始したユーザ、アプリケーション、またはプロセスが表示されます。



このボタンをクリックすると、スキヤン済みオブジェクトのリストが表示されます。



このボタンをクリックすると、スキヤン済みオブジェクトのリストが非表示になります。



このボタンをクリックすると、レポートをTXTファイルで保存するためのウインドウが表示されます。

ファイル脅威対策のレポート

ウインドウ右側のペインに、ファイル脅威対策の動作に関するレポートが表示されます。

日付

この列には、スキヤン済みオブジェクトにアプリケーションがアクセスした日時が表示されます。

パス

この列には、スキヤンしたオブジェクトの元の保存場所へのパスが表示されます。

ステータス

この列には、スキヤンしたオブジェクトの現在のステータスが表示されます。

プログラム名

この列には、スキヤン済みオブジェクトにアクセスしたアプリケーションが表示されます。



このボタンをクリックすると、レポートをTXTファイルで保存するためのウインドウが表示されます。

ウェブ脅威対策のレポート

ウインドウ右側のペインに、ウェブ脅威対策の動作に関するレポートが表示されます。

日付

この列には、Web トラフィックオブジェクトが検知された日時が表示されます。

URL

この列には、ウェブ脅威対策が検知した Web トラフィックオブジェクトが表示されます。検知された Web トラフィックオブジェクトそれぞれについて、検知された Web ページのアドレスが示されます。

ステータス

この列には、検知された Web トラフィック オブジェクトのステータスが表示されます。

プログラム名

この列には、検知された Web トラフィックオブジェクトにアクセスしたプログラムが表示されます。



このボタンをクリックすると、レポートをTXTファイルで保存するためのウインドウが表示されます。

メール脅威対策のレポート

ウインドウ右側のペインに、メール脅威対策の動作に関するレポートが表示されます。

日付

この列には、メールで感染したオブジェクトが検知された日時が表示されます。

パス

この列には、感染したオブジェクトが検出されたメールに関する情報が表示されます。

ステータス

この列には、感染したオブジェクトの検知後に **Kaspersky Endpoint Security** が実行した処理が表示されます。

プログラム名

この列には、メールクライアント名が表示されます。



このボタンをクリックすると、レポートをTXTファイルで保存するためのウインドウが表示されます。

ネットワーク脅威対策のレポート

ウインドウ右側のペインに、ネットワーク脅威対策の動作に関するレポートが表示されます。

日付

この列には、コンピュータで危険なネットワーク活動が検知された日時が表示されます。

IP アドレス

この列には、検知された危険なネットワーク活動の発生源であるコンピュータの **IP アドレス**が表示されます。

ステータス

この列には、危険なネットワーク活動をの検知後に **Kaspersky Endpoint Security** が実行した処理が表示されます。

攻撃種別

この列には、検知されたネットワーク攻撃の種別が表示されます。

ローカルポート

この列には、侵入が試みられたローカルポートの番号が表示されます。

プロトコル

この列には、攻撃の実行に使用したプロトコルの種別が表示されます。



このボタンをクリックすると、レポートをTXTファイルで保存するためのウインドウが表示されます。

Endpoint Detection and Response レポート

ウインドウ右側のペインに、**Endpoint Detection and Response** コンポーネントの動作に関するレポートが表示されます。

日付

この列には、イベントの日付と時刻が表示されます。

イベント

この列には、イベントのステータスが表示されます。



このボタンをクリックすると、レポートをTXTファイルで保存するためのウインドウが表示されます。

ファイアウォールのレポート

ウインドウ右側のペインに、ファイアウォールの動作に関するレポートが表示されます。

日付

この列には、イベントの日付と時刻が表示されます。

イベント

この列には、イベントのステータスが表示されます。



このボタンをクリックすると、レポートをTXTファイルで保存するためのウインドウが表示されます。

脆弱性攻撃ブロックのレポート

ウインドウ右側のペインに、脆弱性攻撃ブロックの動作に関するレポートが表示されます。

日付

この列には、イベントの日付と時刻が表示されます。

イベント

この列には、イベントのステータスが表示されます。



このボタンをクリックすると、レポートをTXTファイルで保存するためのウインドウが表示されます。

デバイスコントロールのレポート

ウインドウ右側のペインに、デバイスコントロールの動作に関するレポートが表示されます。

日付

この列には、イベントの日付と時刻が表示されます。

イベント

この列には、イベントのステータスが表示されます。



このボタンをクリックすると、レポートをTXTファイルで保存するためのウインドウが表示されます。

システムウォッチャーレポート

ウインドウ右側のペインに、システムウォッチャーの動作に関するレポートが表示されます。

日付

この列には、イベントの日付と時刻が表示されます。

イベント

この列には、イベントのステータスが表示されます。



このボタンをクリックすると、レポートをTXTファイルで保存するためのウインドウが表示されます。

サポートウインドウ

このウインドウには、次の情報が表示されます：

- 定義データベースの公開日
- 現在 Kaspersky Endpoint Security で使用している定義データベースの公開日
- コンピュータにインストールされているオペレーティングシステムのバージョン

テクニカルサポート

このボタンをクリックすると、テクニカルサポートのよくある質問と回答のページが表示されます。カスペルスキーの担当者が公開した、Kaspersky Endpoint Security に関する記事を閲覧できます。

コミュニティ

このボタンをクリックするとコミュニティが開き、Kaspersky Endpoint Security についてカスペルスキーのエキスパートや他のユーザとディスカッションできます。

閉じる

このボタンをクリックすると、ウインドウが閉じます。

〔証明書の設定〕 ウインドウ

〔全般〕 タブでは、Mozilla Firefox ブラウザで暗号化された HTTPS トラフィックをチェックするための証明書ストアを選択できます。

- システムルートキーチェーン（推奨）
- Mozilla Firefox のブラウザー設定の証明書ストア

この場合、Kaspersky Endpoint Security 証明書を Mozilla Firefox ブラウザの証明書ストアに手動で追加する必要があります。詳細は、[「Kaspersky Endpoint Security 証明書を Mozilla Firefox 証明書ストアに追加する方法」](#)を参照してください。

〔信頼できる証明書〕 タブで信頼済みルート証明書のリストを作成し、そのリストにあるサーバへの接続時に通知が表示されないように設定することができます。

信頼済みルート証明書のリストは、既定では空です。



このボタンをクリックすると、信頼済みと判断される証明書を追加するダイアログが表示されます。



このボタンをクリックすると、選択した証明書が信頼する証明書のリストから削除されます。

証明書の名前

この列には、信頼済みルート証明書の名前が表示されます。

キャンセル

このボタンをクリックすると、変更を保存せずにウインドウを閉じます。

保存

このボタンをクリックすると、現在の信頼済みルート証明書のリスト保存し、ウインドウを閉じます。

〔証明書を検証〕 ウインドウ

証明書を表示

このボタンをクリックすると、証明書の情報を含むシステムウインドウが表示されます。

キャンセル

このボタンをクリックすると、ウインドウが閉じます。

信頼済みに追加する

このボタンをクリックすると、証明書が信頼済み証明書のリストに追加されます。これにより、対応するサーバに通知なしで接続できるようになります。

接続

このボタンをクリックすると、サーバへ接続します。

注意：使用可能なボタンは、証明書の種別により異なります。

〔証明書の選択〕 ウインドウ

使用できる証明書の一覧

証明書に隣接するチェックボックスをオンにして、サーバーへの接続時にこの証明書を使用します。

証明書を表示

このボタンをクリックすると、証明書の情報を含むシステムウインドウが表示されます。

キャンセル

このボタンをクリックすると、ウインドウが閉じます。

続行

このボタンをクリックすると、選択した証明書を使用してサーバーへの接続を続行します。